Europäisches Patentamt
European Patent Office
Office européen des brevets

European Patent Office
Data Protection Register

According to Article 32 European Patent Office Data Protection Rules (EPO DPR), the EPO has the legal obligation to keep the Record of processing activities in a Register. The Register is managed by the Data Protection Office (DPO) and the delegated controllers remain responsible for the content of the Records.

The present document provides for information on the processing of personal data concerning external data subjects, on their purpose and conditions of such processing operations. This document is regularly updated to include new or new version of existing Records.

The Records included herein provide at least the following information:

- the name and contact details of the controller and/or the delegated controller, the Data Protection Officer and, where applicable, the processor and the joint controller;
- the purposes of the processing;
- a description of the categories of data subjects and of the categories of personal data;
- the categories of recipients to which the personal data have been or will be disclosed, including recipients in third countries or other international organisations;
- where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards;
- where possible, the envisaged time limits for erasure of the different categories of data;
- where possible, a general description of the technical and organisational security measures referred to in Article 33 EPO DPR.

Additional information about the processing operations can be found in the related data protection statement available on the EPO Data protection and privacy notice, under the Section “Information on the processing of personal data in EPO products and services”.

If you have questions concerning specific processing activities, you wish to contact the relevant delegated controllers or the Data Protection Officer, or to report a personal data breach, please send an email to DPOexternalusers@epo.org

List of Record of processing activities under Article 32 EPO DPR:

ID	Name
19	Processing of personal data within the framework of the Data Protection Office tasks, duties and activities
21	Collection and management of contact lists of Brussels' stakeholders
22	Internal audit
26	Selection of members of SACEPO (Standing Advisory Committee before the EPO) and its working parties
39	Delivery of Patent Knowledge related data
40	Patent Knowledge News
41	European Publication Server
42	PISE Services
43	EPO hosted PK services
45	Patent Knowledge Web Shop
46	PK User Support
47	PATLIB
50	Off-site storage of PGP paper files
57	Tender procedures and agreements between external supplier and the EPO
64	List of contact names to support settlement and safekeeping of securities
65	List of contact names to support dealing in financial securities and cash management
66	List of contact names to support use of RFPSS investment management platform.
68	Customer Services Management (CSM)
75	European Patent Register
76	SACEPO meetings
77	Disciplinary procedures against professional representatives before the EPO
78	Selection of members of the Disciplinary board of the Office
79	Organisation of meetings with the US Bar-EPO liaison Committee
81	Legal advice on contractual, (pre-)litigation and other general matters by Directorate 5.2.4 – Contract law and litigation
82	Maintenance of List of professional representatives
83	Activities related to pre-litigation and litigation on civil service matters where the Administrative Council is competent appointing authority
86	Microsoft Office365 applications
94	Vaccination campaigns
95	Processing of personal data within the framework of the European and International Cooperation units' tasks, duties and activities
96	House Ban List
103	Processing of personal data within the framework of approval of formal documentation by the President's Office
120	Study on European Patent Applications to produce statistics on the gender of inventors.
122	Learning Management System
125	Fitness & Vitality Service
126	EP Full Text for Text Analytics
127	Open Patent Services
129	Post grant contact management
134	Official Publications
137	Federated Services
144	Automated Number Plate Recognition (ANPR) system

145	Video Surveillance Systems
148	Workflows in the Patent Workbench
150	Amicable Settlement Attempt
159	Access Control and Card Management Systems - DG4 -PD44 - General Administration
161	Consultations and assessments of the capacity to work of staff by the EPO Medical Services
164	Identity Management through AD and Azure AD
165	Microsoft Defender for Endpoint
166	Accident reporting
167	Medical certificates/consultancy registration process
175	Employee Assistance Programme (EAP)
177	Physiotherapy service
178	Registration of Munich staff's children in crèches subsidised by the Office
179	Consultation with the Ombuds Office - external clients
180	Personal Evacuation Emergency Plan (PEEP)
182	Disposal of e-waste
184	Applications and patents related Legal advice
205	Splunk
211	Booking process for office space and/or electrical charging station - SmartWay2 system - PD 4.4 General Administration
212	Contact Center Solution - Anywhere 365
215	Videoconferencing via Zoom
217	EQE - European Qualifying Examination
225	Staff requests that require medical assessments by the EPO Medical Services
227	Identity Management through Okta
229	Legal Affairs cooperation with CPVO - Joint Seminar
230	Email usage
232	Institutional issues and matters relating to the Legal division and the Unitary Patent Division - provision of legal advice
233	Legal practitioners' list and its maintenance
234	User Consultation on Guidelines for Examination
235	Associations' lists maintenance
239	Dispute settlement activities in national proceedings or arbitration context
241	Central Fee Payment
243	“MyEPO Portfolio” online service for parties to proceedings before the EPO (PGP)
244	European, international and PCT related legal advice (D 5.2.2)
246	Archives Legal Affairs
247	Mattersphere Case Management System in Legal Affairs/PD5.2
249	Personal data processing related to team and service quality management in the interpreting area
250	Convergence of practice (SP2023 Programme 4.4.2)
251	General Authorisations maintenance
252	Programme 4.5.3 “Improving the quality of PCT products and services”
254	EPO Academy
255	European Patent Administration Certificate (EPAC)
256	Organisation of Meetings between Legal Affairs and EPI
268	Personal data processing in editing/translation services-DG4 - PD44 - General Administration | European Patent Office | Germany
269	Document design services
274	Invoicing

277	Data Protection Board - Case management for complaints lodged by external data subjects
281	Personal Data processing performed within the Logistic Centre activities - officewide -DG4 - PD 44 - General Administration
283	EPO E-Learning Centre
286	Security documentation storage
288	Job shadowing
291	Processing of personal data within the framework of the Data Protection Board tasks, duties and activities
292	Long-Term Care Insurance
293	IP5 Offices and Trilateral Offices websites
295	Search tool for National Patent Offices
298	Bot protection service (Friendly Captcha)
300	Processing of International Labour Organisation Administrative Tribunal (ILOAT) complaints for external data subjects
302	Internal Appeals Procedure for External Data Subjects
304	Data Protection Board Complaints Procedure for External Data Subjects
305	Amicable Settlement Attempt for External Data Subjects
309	Disciplinary Procedure for External Data Subjects
310	Professional Incompetence Procedure for External Data Subjects
318	User satisfaction surveys on search services, on examination services, final actions and publication as well as on opposition services
320	Mass email distribution list management
345	Quantifying the user-specific usage of MyEPO Portfolio service and publishing the Top Digital Champions of the MyEPO Portfolio service on epo.org
356	Communication sent and social activities organised for staff by Amicale Berlin
358	Processing of personal data by the EPO Observatory on Patent and Technology
360	Personal data processing for insurance purposes and damage claim handling
362	External general tasks and activities carried out by PD02
365	User Consultation 2023 - amendments RPBA
368	“EPO Contingency Upload Service” for the parties to proceedings before the EPO (PGP)
376	Activities organised by Amicale Munich
377	Activities organised by Amicale Vienna
378	Activities organised by Amicale the Hague
383	Management of the MICADO Address Book (MAB)
386	Archiving of Council Secretariat’s documents which include personal data
406	EPO Together
417	Constitution of the Jury Members’ Panel for the European Inventor Award and Young Inventors prize
418	User Experience (UX) research on EPO software applications
420	EPO Art collection management
426	Management of the MICADO Address Book (MAB) - SC
433	Archiving of Select Committee’s documents which include personal data
434	Contractor management (creation, on/offboarding, deletion of EPO external contractors)
435	Formal complaint and feedback
438	Digitisation of incoming paper documents, paper file related internal tasks and preparatory work for DG1 formalities officers
440	EPO outreach activities
441	Procurement activities
443	Legal Business Partner brand
446	Patent Index
457	Personal data collected in the context of building projects for obtaining Building Permits at EPO Sites

458	PGP paper files in C-Lab
460	Management of personal data in building permit applications
462	EPO Legal Interactive Platform
463	Workflow, Data and Knowledge management based on EPO ServiceNow capabilities
466	RFPSS Recording MS Teams trainings
471	Deep Tech Finder Application
473	Meetings and events managed by PDComm
474	European Inventor Award (EIA) and Young Inventors Prize (YIP)
496	EPO's email newsletters, alerts and subscription centre

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 19

Name Processing of personal data within the framework of the Data Protection Office tasks, duties and activities

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG0 - 07 - Data Protection Office

External processors

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

OpenText

External processors	
Name OpenText	

OpenText

External processors	
Name OpenText	

Microsoft

External processors

Name
Microsoft

Microsoft

External processors
Name
Microsoft

OneTrust

External processors
Name
OneTrust

OneTrust

External processors
Name
OneTrust

Microsoft

External processors
Name
Microsoft

Description of the processing

Description The EPO's Data Protection Office (DPO) processes personal data in order to carry out the tasks and duties assigned to it by the Service Regulations for permanent and other employees of the EPO (Service Regulations), the DPR, other rules, administrative instructions and decisions adopted by the President of the Office and additional operational documents governing the processing of personal data at the EPO.

In the performance of its tasks, the DPO may process any category of personal data (including special categories of personal data) provided by EPO staff members or externals regarding themselves or third parties. It includes information exchanged such as the description of concerns, personal case, circumstances, description of facts, opinions, assessments, etc.

Personal data may be stored in one or more document management tools used by the DPO to perform its tasks, namely on the EPO's servers and/or in Microsoft Office cloud systems and/or in OpenText and/or in the Data Protection Tool (DP Tool):

-all data subjects' enquiries, DPO opinions, advice, recommendations and consultations, and related communications (together with supplementary documentation, as the case may be) received or sent by the DPO are stored in Outlook in folders separated by year and/or on SharePoint 2019 and are only accessible to authorised staff. They are afterwards archived in MatterSphere with a unique identifier assigned to them
- personal data in relation to records of processing activities are stored in the DP Tool
- documents (e.g. drafts of operational documents, awareness-raising materials) are stored in the document management tool OpenText.

For more information regarding the processing of personal data in these tools, please refer to the dedicated record(s).

The DPO processes personal data in the frame of the Data Protection Liaisons (DPLs) network. DPLs are appointed by each delegated controller to be their contact point in relation to data protection matters.

The DPO registers the presence of invitees in meetings and events organised by the DPO (for example trainings, DPLs meetings) for the purpose of establishing the list of attendees for the minutes of the meeting or event and for monitoring purposes.

The DPO may also be requested by the Data Protection Board (DPB) to provide support, to that extent the DPO may process, on a strictly need-to-know basis, personal data such as the details of the data subject filing a complaint, personal data contained in allegations, and other categories of personal data depending on the case. For more information on the processing of personal data by the DPB, Please refer to the relevant record.

The processing is not intended to be used for any automated individual decision-making.

Data Retention Personal data will be kept only for the time needed to achieve the purpose(s) for which they are processed.

Personal data related to records inserted in the DP Tool/SharePoint 2019 will be stored for as long as the processing is operational. After that date, the record will be deleted from the public Register but archived for a period of 5 years for reasons of possible formal appeals and litigation procedures.

Personal data related to co-operation with external and internal stakeholders will be stored in the document management tool(s) for a maximum of 5 years after the closure of the case.

Purpose of Processing carrying out data protection investigations and audits, raising awareness/ providing training on data protection matters, providing opinions, advice, recommendations and responses regarding consultations received from the relevant controller, delegated controllers, processors or any body set up under Article 2 of the Service Regulations, offering support to the DPB in carrying out its function under the DPR, assisting organisational units with (internal or external) data subjects' enquiries (meaning queries, requests to exercise data subject' rights, requests for review by the delegated controller, complaints of alleged infringement of the DPR, including potential reports on personal data breaches), co-operating with other organs of the European Patent Organisation (i.e. the Administrative Council), European Union institutions, bodies, offices and agencies and/or other international organisations, - maintaining the Data Protection Register within the DP Tool and SharePoint 2019 (https://sharepoint2019.internal.epo.org/sites/DPOREG/Lists/DPORegisterintranet/AllItems.aspx) o Records involving the processing of external data subjects' personal data are publicly accessible on the EPO website (https://documents.epo.org/projects/babylon/eponet.nsf/0/B8C31CF8AC6C19D8C12587AD002F98CB/$FILE/data_protection_register_en.pdf) . The only personal data processed in this context are the cookies used on the EPO website., assessing risks for individuals resulting from personal data breaches, managing the DPLs network, monitoring the attendance of invitees to meetings organized by the DPO

Personal data related to DPO opinions, advice, recommendations, consultation and related communications will be stored in the document management tool(s) for a maximum of 5 years after the closure of the consultation or provision of the opinion, advice or recommendation.

Personal data related to data subject enquiries (internal and external) will be stored in the document management tool(s) for a maximum of 10 years after the closure of the enquiry.

Personal data related to data protection investigations will be stored in the document management tool(s) for 10 years after the closure of the investigation.

Personal data related to audits will be stored in the document management tool(s) for 5 years after finalisation of the final audit report.

Personal data related to the assessment of personal data breaches are stored in the document management tool(s) for 10 years after finalisation of the data breach report.

Personal data processed to provide support and/or opinions, or recommendations in relation to Article 49 DPR (request for review by the delegated controller), Article 50 DPR (legal redress) and Article 51 DPR (incidental data protection request during internal appeal proceedings – only relevant for EPO staff) will be stored in the document management tool(s) for 10 years after finalisation of the opinion.

The retention period of the personal data contained in the documents received by the DPO, in the performance of its tasks, is also defined in the records of operational processes supported by those documents.

In the event of a formal appeal/litigation, all data held at the time the formal appeal/litigation was initiated will be retained until the proceedings have been closed.

Personal data related to records inserted in the EPO Data Protection Register will be stored as long as the processing is operational.

After that date the record will be deleted from the Register but archived the period of 5 years for reasons of possible legal appeal procedures.

Personal data related to consultations, complaints, requests from the data subjects and data protection audits will be archived in the document management tool for the period of 5 years.

Personal data related to complaints filed with the DPB are to be kept for:
i. a maximum of 5 years after the closure for inadmissible complaints
ii. a maximum of 10 years after closure of an admissible complaint.

Personal data related to the personal data breaches are to be kept for 10 years after closure of the case.

The retention period of the personal data contained in the documents is also defined in the records of the operational processes supported by those documents.

The records' retention schedule also indicates the subsequent actions at the end of the administrative retention period on the basis of the potential historical value of documents and files. These actions include elimination of certain data, sampling or selection and long-term preservation of the documents and cases identified as archives.

Data subjects and categories of personal data	Contractors
Applications' Log	
SAP Logs	
Sensory and Electronic Information	
Audio Information	Electronic Information
Thermal Information	Time stamps from their access to the buildings
Visual Information	
Building area and site	
Building area and site	
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name
Gender	Height
Surname	Marital Status
Nationality	Picture
Racial or Ethnic Origin	Religion/Religious Beliefs
Sexual Orientation	Signature
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
Project management experience	
General	
Any other information	Assessment and legal opinions
Input provided during the deliberation and decision-making process	Nomination justificative

User association	
Workplace Welfare	
Records of Personal Properties	
Contact Information	
Contact Details	Country
Emergency Contact Details	Home Address
Mobile Phone Number	Personal Email
Phone Numbers	Previous Residence Address
Teleworking address	Working email address
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
IDP	Instructor related data
Learning external events	Learning history
Learning plan	Social learning inputs
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Health Insurance Information	
Insurance Policy Information	Unique Identifier for Subscriber
System Logs	
File data (name, size and/or hash)	Ports
Registry data	Running Processes
Ticketing	
Ticket related data	
Physical and/or Digital Identifiable Assets	
Digital Certificate	Operating System Version
Smart Card Number	Workstation Serial Number

Workstation's Hostname (Physical or Virtual)	Workstation's Network Adapter MAC address
Biometric	
Body temperature	Facial Recognition
Fingerprint	Voice Recognition
Online invigilation data	
Audio input	Webcam captures
Background Checks	
Criminal History	Criminal Records
Drug Test Results	Reference or Background Checks
Employment Information	
Appeals Records Information	Assessment and legal opinions
Benefits and Entitlements Data	Business Unit Division
Company Entity	Contract Type
Corporate Credit or Debit Card Numbers	Department name and/or number
Disciplinary Action	Duration of employment
End Date	End Date and Reason for Termination
EPO access badge number	Exit Interview and Comments
Grade	Grievances and Complaints
Hours of Work	Job Application Details
Job Title Role	Language preference (of communication)
Line Reporting Manager	Membership in a EPO Staff Committee
Military Status	Office Location
Performance Rating	Personnel Number
Previous Work History	Record of Absence/Time Tracking/Annual Leave
Record of Maternity Leave	Room Number
Salary	Start Date
Weight	

Unknown	
EPO badge validity	Identification of which membership is envisaged
Price list for discounts	
Geolocation	
Geolocation Information	
Network/application Interaction Data	
Session content	Session details
Session metadata	
Health Data	
Dietary requirements	Health Data
Mobility needs	
Professional Experience & Affiliations	
Affiliation	CV
Political Affiliation and Activities	Professional Memberships
Qualifications Certifications	Trade Union Membership
Examination content data	
Examination marks	Examination result
Financial	
Bank Account Information	Bank Account Number
Bank Statements	Bonus Payments
Compensation Data	Credit Card Number
Credit History	Debit Card Number
Fund Reservation Requests	Information on home loans
Insurance Information	Routing Number
Browsing Information	
Browser type	Browsing Time
Cookie Information	IP Address

Network Interaction History	Website History
User Account Information	
Account Age	Account Number
Account Password	Password
User ID	
Government Identifiers	
Driving Licence Number	National Identification Number
National Identity Card Details	Passport Number
Social Security Number	

Employees

Applications' Log	
SAP Logs	
Sensory and Electronic Information	
Audio Information	Electronic Information
Thermal Information	Time stamps from their access to the buildings
Visual Information	
Building area and site	
Building area and site	
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name
Gender	Height
Surname	Marital Status

Nationality	Picture
Racial or Ethnic Origin	Religion/Religious Beliefs
Sexual Orientation	Signature
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
Project management experience	
General	
Any other information	Assessment and legal opinions
Input provided during the deliberation and decision-making process	Nomination justificative
Personal Information in SAP	Sensitive Personal Data in SAP
Special Categories of Data in SAP	User association
Workplace Welfare	
Records of Personal Properties	
Contact Information	
Contact Details	Country
Emergency Contact Details	Home Address
Home Leave Address	Mobile Phone Number
Personal Email	Phone Numbers
Previous Residence Address	Teleworking address
Working email address	
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
Diagnostic tools' results	IDP
Instructor related data	Learning external events
Learning history	Learning plan
Ratings	Social learning inputs

Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Health Insurance Information	
Insurance Policy Information	Unique Identifier for Subscriber
System Logs	
File data (name, size and/or hash)	Ports
Registry data	Running Processes
Ticketing	
Ticket related data	
Physical and/or Digital Identifiable Assets	
Digital Certificate	Operating System Version
Smart Card Number	Workstation Serial Number
Workstation's Hostname (Physical or Virtual)	Workstation's Network Adapter MAC address
Biometric	
Body temperature	Facial Recognition
Fingerprint	Voice Recognition
Online invigilation data	
Audio input	Webcam captures
Background Checks	
Criminal History	Criminal Records
Drug Test Results	Reference or Background Checks
Employment Information	
Appeals Records Information	Assessment and legal opinions
Benefits and Entitlements Data	Business Unit Division
Company Entity	Contract Type
Corporate Credit or Debit Card Numbers	Department name and/or number

Disciplinary Action	Duration of employment
End Date	End Date and Reason for Termination
EPO access badge number	Exit Interview and Comments
Grade	Grievances and Complaints
Hours of Work	Job Application Details
Job Group	Job Title Role
Language preference (of communication)	Line Reporting Manager
Membership in a EPO Staff Committee	Military Status
Office Location	Performance Rating
Personnel Number	Previous Work History
Record of Absence/Time Tracking/Annual Leave	Record of Maternity Leave
Rewards history	Room Number
Salary	Start Date
Weight	
Unknown	
EPO badge validity	Identification of which membership is envisaged
Price list for discounts	
Geolocation	
Geolocation Information	
Network/application Interaction Data	
Session content	Session details
Session metadata	
Health Data	
Dietary requirements	Health Data
Mobility needs	
Professional Experience & Affiliations	
Affiliation	CV

Political Affiliation and Activities	Professional Memberships
Qualifications Certifications	Trade Union Membership
Examination content data	
Examination marks	Examination result
Family Information	
Child's Level/Year of Studies	Child's School Enrolment Date Start
Children's Names	Child's birthday
Composition of the family (number of dependent children/persons)	Parents' Names
Spouse's information	Spouse's name
Financial	
Bank Account Information	Bank Account Number
Bank Statements	Bonus Payments
Compensation Data	Credit Card Number
Credit History	Debit Card Number
Fund Reservation Requests	Information on home loans
Insurance Information	Routing Number
Browsing Information	
Browser type	Browsing Time
Cookie Information	IP Address
Network Interaction History	Website History
User Account Information	
Account Age	Account Number
Account Password	Password
User ID	
Government Identifiers	
Car registration documents	Driving Licence Number
National Identification Number	National Identity Card Details

Passport Number	Social Security Number

Externals

Applications' Log	
SAP Logs	
Sensory and Electronic Information	
Audio Information	Electronic Information
Time stamps from their access to the buildings	Visual Information
Building area and site	
Building area and site	
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name
Gender	Surname
Nationality	Picture
Signature	
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
Project management experience	
General	
Any other information	Input provided during the deliberation and decision-making process
Nomination justificative	User association
Contact Information	

Contact Details	Country
Emergency Contact Details	Home Address
Mobile Phone Number	Personal Email
Phone Numbers	Working email address
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
IDP	Instructor related data
Learning external events	Learning history
Learning plan	Ratings
Social learning inputs	
European Patent Register Data	
Address	Data provided by the data subjects
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
System Logs	
File data (name, size and/or hash)	Ports
Registry data	Running Processes
Ticketing	
Ticket related data	
Physical and/or Digital Identifiable Assets	
Digital Certificate	Operating System Version
Smart Card Number	Workstation Serial Number
Workstation's Hostname (Physical or Virtual)	Workstation's Network Adapter MAC address
Biometric	
Facial Recognition	Voice Recognition
Online invigilation data	

Audio input	Webcam captures
Employment Information	
Business Unit Division	Company Entity
Contract Type	Corporate Credit or Debit Card Numbers
Department name and/or number	Duration of employment
End Date	EPO access badge number
Hours of Work	Job Title Role
Language preference (of communication)	Membership in a EPO Staff Committee
Office Location	Previous Work History
Record of Maternity Leave	
Unknown	
EPO badge validity	Identification of which membership is envisaged
Price list for discounts	
Network/application Interaction Data	
Session content	Session details
Session metadata	
Health Data	
Dietary requirements	Health Data
Mobility needs	
Professional Experience & Affiliations	
Affiliation	CV
Political Affiliation and Activities	Professional Memberships
Qualifications Certifications	
Examination content data	
Examination marks	Examination result
Financial	
Bank Account Information	Bank Account Number

Credit Card Number	Debit Card Number
Fund Reservation Requests	Information on home loans
Insurance Information	
Browsing Information	
Browser type	Browsing Time
Cookie Information	IP Address
Network Interaction History	Website History
User Account Information	
Account Age	Account Number
Account Password	
Government Identifiers	
National Identity Card Details	Passport Number

Former Employees

Applications' Log	
SAP Logs	
Sensory and Electronic Information	
Audio Information	Electronic Information
Thermal Information	Time stamps from their access to the buildings
Visual Information	
Building area and site	
Building area and site	
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name

Gender	Height
Surname	Marital Status
Nationality	Picture
Racial or Ethnic Origin	Religion/Religious Beliefs
Sexual Orientation	Signature
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
Project management experience	
General	
Any other information	Input provided during the deliberation and decision-making process
Nomination justificative	Personal Information in SAP
Sensitive Personal Data in SAP	Special Categories of Data in SAP
User association	
Workplace Welfare	
Records of Personal Properties	
Contact Information	
Contact Details	Country
Emergency Contact Details	Home Address
Home Leave Address	Mobile Phone Number
Personal Email	Phone Numbers
Previous Residence Address	Teleworking address
Working email address	
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
IDP	Instructor related data
Learning external events	Learning history

Learning plan	Social learning inputs
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Health Insurance Information	
Insurance Policy Information	Unique Identifier for Subscriber
System Logs	
File data (name, size and/or hash)	Ports
Registry data	Running Processes
Ticketing	
Ticket related data	
Physical and/or Digital Identifiable Assets	
Digital Certificate	Operating System Version
Smart Card Number	Workstation Serial Number
Workstation's Hostname (Physical or Virtual)	Workstation's Network Adapter MAC address
Biometric	
Body temperature	Facial Recognition
Fingerprint	Voice Recognition
Online invigilation data	
Audio input	Webcam captures
Background Checks	
Criminal History	Criminal Records
Drug Test Results	Reference or Background Checks
Employment Information	
Appeals Records Information	Benefits and Entitlements Data
Business Unit Division	Company Entity
Contract Type	Corporate Credit or Debit Card Numbers

Department name and/or number	Disciplinary Action
Duration of employment	End Date
End Date and Reason for Termination	EPO access badge number
Exit Interview and Comments	Grade
Grievances and Complaints	Hours of Work
Job Application Details	Job Group
Job Title Role	Language preference (of communication)
Line Reporting Manager	Membership in a EPO Staff Committee
Military Status	Office Location
Performance Rating	Personnel Number
Previous Work History	Record of Absence/Time Tracking/Annual Leave
Record of Maternity Leave	Rewards history
Salary	Start Date
Weight	
Unknown	
EPO badge validity	Identification of which membership is envisaged
Price list for discounts	
Geolocation	
Geolocation Information	
Network/application Interaction Data	
Session content	Session details
Session metadata	
Health Data	
Dietary requirements	Health Data
Mobility needs	
Professional Experience & Affiliations	
Affiliation	CV

Political Affiliation and Activities	Professional Memberships
Qualifications Certifications	Trade Union Membership
Examination content data	
Examination marks	Examination result
Family Information	
Children's Names	Parents' Names
Spouse's information	Spouse's name
Financial	
Bank Account Information	Bank Account Number
Bank Statements	Bonus Payments
Compensation Data	Credit Card Number
Credit History	Debit Card Number
Fund Reservation Requests	Information on home loans
Insurance Information	Routing Number
Browsing Information	
Browser type	Browsing Time
Cookie Information	IP Address
Network Interaction History	Website History
User Account Information	
Account Age	Account Number
Account Password	Password
User ID	
Government Identifiers	
Driving Licence Number	National Identification Number
National Identity Card Details	Passport Number
Social Security Number	

Prospective Employees

Applications' Log	
SAP Logs	
Sensory and Electronic Information	
Time stamps from their access to the buildings	
Building area and site	
Building area and site	
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name
Gender	Height
Surname	Marital Status
Nationality	Picture
Religion/Religious Beliefs	Signature
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
Project management experience	
General	
Any other information	Input provided during the deliberation and decision-making process
Nomination justificative	User association
Contact Information	
Contact Details	Country
Emergency Contact Details	Home Address
Mobile Phone Number	Personal Email

Phone Numbers	Working email address
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
IDP	Instructor related data
Learning external events	Learning history
Learning plan	Social learning inputs
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
System Logs	
File data (name, size and/or hash)	Ports
Registry data	Running Processes
Ticketing	
Ticket related data	
Physical and/or Digital Identifiable Assets	
Operating System Version	Workstation Serial Number
Workstation's Hostname (Physical or Virtual)	Workstation's Network Adapter MAC address
Online invigilation data	
Audio input	Webcam captures
Background Checks	
Criminal History	Criminal Records
Drug Test Results	Reference or Background Checks
Employment Information	
Benefits and Entitlements Data	Business Unit Division
Company Entity	Contract Type
Department name and/or number	Duration of employment
End Date	End Date and Reason for Termination

EPO access badge number	Grade
Job Application Details	Job Group
Job Title Role	Language preference (of communication)
Line Reporting Manager	Membership in a EPO Staff Committee
Military Status	Office Location
Performance Rating	Previous Work History
Record of Maternity Leave	Rewards history
Salary	Start Date
Weight	
Unknown	
EPO badge validity	Identification of which membership is envisaged
Price list for discounts	
Network/application Interaction Data	
Session content	Session details
Session metadata	
Health Data	
Dietary requirements	Health Data
Mobility needs	
Professional Experience & Affiliations	
Affiliation	CV
Political Affiliation and Activities	Professional Memberships
Qualifications Certifications	
Financial	
Fund Reservation Requests	Information on home loans
Examination content data	
Examination marks	Examination result
Browsing Information	

Browser type	
User Account Information	
Account Age	Account Number
Account Password	Password
Government Identifiers	
National Identity Card Details	Passport Number

Recipient of the personal data

Recipients of the data Where strictly necessary to perform its tasks, personal data may be disclosed on a need-to-know basis to the staff working in the DPO, to the relevant controller, the delegated controller(s), the DPLs and to any other authorised staff. Personal data will only be shared with authorised persons responsible for the necessary processing operations. They will not be used for any other purposes or disclosed to any other recipients.

Personal data processed in the DP Tool may be disclosed to a third-party service provider for maintenance and support purposes of the DP tool.

Personal data may be disclosed to the Data Protection Board when the DPO's support is requested.

In addition:

- in the case of data subject (internal or external) enquiries, personal data may be disclosed to the delegated controllers responsible for the processing operation related to the enquiry. Strictly necessary personal data may be shared with other units (such as a technical team or human resources) as necessary to collect and compile relevant information to respond to the enquiry
- in the case of data breaches, personal data may be disclosed to the President of the Office, the delegated controller, the processor and authorised staff as necessary to handle the breach
- in the case of an investigation under Article 43(1)(d) and (2) DPR, personal data may be disclosed to the person who commissioned the data protection investigation and/or the President of the Office, the delegated controller, the processor or the body set up under the legal provisions of the European Patent Organisation
- in the case of an audit under Article 43(1)(d), personal data may be disclosed to the President of the Office, the delegated controller (auditee) and the processor
- in the case of an opinion requested from the DPO under Article 49(2) DPR, personal data may be disclosed to the delegated controller who received the request for review
- in the case of an opinion requested from the DPO under Article 51 DPR, personal data may be disclosed to the body under the Service Regulations advising the appointing authority and to the appointing authority
- in the context of co-operation with external and internal stakeholders, personal data may be disclosed to authorised staff members of the DPO, the President of the Office or the relevant delegated controller.

Purpose of sharing - to perform the DPO's tasks and duties
- to provide support to the DPB upon request
- to co-operate with external and internal stakeholders

Depending on the case, personal data might be disclosed to different recipients:

- in the case of an investigation according to Articles 43 (1)(d) and 43(2) DPR, personal data might be disclosed to the person who commissioned the data protection investigation or the President, the delegated controller, the processor or the body set up under the legal provisions of the European Patent Organisation;
- in the case of an opinion requested to the DPO according to Article 49(2) DPR, personal data might be disclosed to the delegated controller that received the request for review;
- in the case of an opinion requested to the DPO according to Article 51 DPR, personal data may be disclosed to the body under the Service Regulations advising the appointing authority and the appointing authority.

In the context of data protection audit, personal data (such as performance indicators, privacy metrics or DPO audit reports and follow up reports), might be disclosed to the President and the Presidential Office. Audit reports and follow up reports might be published on the DPO corner on Intranet.

Personal data might be disclosed to the DPB when the support of the DPO is requested.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards, Data Protection EU Comm Standard Contractual Clauses, Derogation in accordance with Art. 10 DPR

Country where data might be transferred - Processor (Vendors) TRE Thomson Reuters - Luxembourg, Microsoft - United States, OneTrust - United States, OpenText - United Kingdom

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, International cooperation activities

Derogations Art. 10 DPR The transfer is necessary for the performance of a task in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning, or to perform obligations arising from its duty of co-operation with the contracting states

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 21

Name Collection and management of contact lists of Brussels' stakeholders

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG0 - 01 - President`s Office - Vice-President

Description of the processing

Description The source of the personal data of Brussels' stakeholders is either publicly available information or information retrieved through personal contact with organisations of interest. The data thus collected is entered in the delegated controller's contacts data base. The personal data from these lists is used for invitations to EPO events or information on EPO activities.

As for the destruction of the data, we update our database regularly considering that Brussels based stakeholders usually remain in post for a period of 3 to 5 years.

Data Retention The personal data of the data subjects concerned is kept in the lists as long as they remain Brussels IP stakeholders as defined above. Once the data subjects are not fulfilling these conditions anymore, the personal data is deleted

Purpose of Processing Personal data is processed for the purpose of developing and maintaining a network of formal and informal contacts with Brussels' key players such as the EU Institutions, relevant stakeholders (industry federations, NGOs, law firms, other public entities etc).

Data subjects and categories of personal data

Externals

Sensory and Electronic Information	
Electronic Information	
Contact Information	
Contact Details	Home Address
Personal Email	Phone Numbers

Professional Experience & Affiliations	
Political Affiliation and Activities	Professional Memberships
Personal Identification	
First Name	Full Name
Gender	Surname
Nationality	

Recipient of the personal data

Recipients of the data The EPO Communication Department will have access to limited information of the data subjects stored on the contacts database (name, first name, organisation, position, where applicable Directorate/Department and responsibilities)

Purpose of sharing Need to know basis (to inform data subject on the launch of EPO studies or any EPO activities)

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 22

Name Internal audit

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 42 - People, DG0 - 05 - Administration of Reserve Funds, DG4 - 423 - HR Essential Services, DG4 - 46 - CIO / BIT, DG4 - 45 - CTO / BIT, DG4 - 43 - Welfare & Remuneration, DG4 - 44 - General Administration, DG4 - 421 - Talent Acquisition and Development, DG4 - 422 - People Engagement and Partnership, DG4 - 41 - Finance

Entity Name - Controller (Entities) DG0 - 041 - Internal Audit and Professional Standards - Internal Audit

External processors

OpenText

External processors	
Name OpenText	

Consulting Auditing Firms

External processors	
Name Consulting Auditing Firms	

Microsoft

External processors	
Name Microsoft	

Description of the processing

Description Internal Audit processes personal data to achieve its mission (namely to enhance and protect organisational value by providing risk-based and objective assurance, advice and insight). Internal Audit interviews staff responsible for the audited operations, carries out surveys, analyses documentation and data in information systems. The Internal Audit activities do not typically target natural persons as such. Nevertheless, personal data are inevitably processed during the course of Internal Audit activities (i.e. for the internal audit's planning, fieldwork and follow-up).
As a general rule, the internal audit reports submitted to the President (RFPSS Supervisory Board) are anonymised.

Data Retention The retention period for internal audit working papers is 10 years after the closure of the internal audit cycle.

Purpose of Processing Planning and conducting internal audits, issuing internal audit reports to the President (or the RFPSS Supervisory Board) and following up on the implementation of recommendations.

Data subjects and categories of personal data

Contractors

Contact Information	
Contact Details	Home Address
Phone Numbers	Previous Residence Address
Teleworking address	Working email address
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
IDP	Instructor related data
Learning external events	Learning history
Learning plan	Social learning inputs
Professional Experience & Affiliations	
Professional Memberships	Qualifications Certifications
Financial	
Bonus Payments	Compensation Data
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Background Checks	
Criminal History	Criminal Records
Reference or Background Checks	

Employment Information	
Appeals Records Information	Benefits and Entitlements Data
Business Unit Division	Company Entity
Contract Type	Corporate Credit or Debit Card Numbers
Disciplinary Action	End Date
End Date and Reason for Termination	Exit Interview and Comments
Grade	Grievances and Complaints
Hours of Work	Job Application Details
Job Title Role	Line Reporting Manager
Military Status	Office Location
Performance Rating	Personnel Number
Previous Work History	Record of Absence/Time Tracking/Annual Leave
Salary	Start Date
Personal Identification	
Age	Date of Birth
Disability or Specific Condition	First Name
Full Name	Gender
Height	Surname
Marital Status	Nationality
Signature	
User Account Information	
User ID	
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages

Employees

Contact Information	
Contact Details	Home Address
Home Leave Address	Personal Email
Teleworking address	Working email address
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
IDP	Instructor related data
Learning external events	Learning history
Learning plan	Social learning inputs
Professional Experience & Affiliations	
Professional Memberships	Qualifications Certifications
Trade Union Membership	
Family Information	
Children's Names	Parents' Names
Spouse's information	Spouse's name
Financial	
Bonus Payments	Compensation Data
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Background Checks	
Criminal History	Criminal Records
Reference or Background Checks	
Employment Information	
Appeals Records Information	Benefits and Entitlements Data
Business Unit Division	Company Entity
Contract Type	Corporate Credit or Debit Card Numbers
Disciplinary Action	End Date

End Date and Reason for Termination	Exit Interview and Comments
Grade	Grievances and Complaints
Hours of Work	Job Application Details
Job Title Role	Line Reporting Manager
Military Status	Office Location
Performance Rating	Personnel Number
Previous Work History	Record of Absence/Time Tracking/Annual Leave
Salary	Start Date
Personal Identification	
Age	Date of Birth
Disability or Specific Condition	First Name
Full Name	Gender
Surname	Marital Status
Nationality	Signature
User Account Information	
User ID	
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages

Externals

Contact Information	
Phone Numbers	Working email address
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
IDP	Instructor related data
Learning external events	Learning history
Learning plan	Social learning inputs

Professional Experience & Affiliations	
Professional Memberships	Qualifications Certifications
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Employment Information	
Business Unit Division	Company Entity
Contract Type	Corporate Credit or Debit Card Numbers
End Date	Hours of Work
Job Title Role	Office Location
Previous Work History	
Personal Identification	
Age	Date of Birth
Disability or Specific Condition	First Name
Full Name	Gender
Surname	Nationality
Signature	
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages

Former Employees

Contact Information	
Contact Details	Home Address
Home Leave Address	Phone Numbers
Previous Residence Address	Teleworking address
Working email address	
Learning managements metrics	

Answers to surveys/Assessments/Quizzes	Coach related data
IDP	Instructor related data
Learning external events	Learning history
Learning plan	Social learning inputs
Professional Experience & Affiliations	
Professional Memberships	Qualifications Certifications
Family Information	
Children's Names	Parents' Names
Spouse's information	Spouse's name
Financial	
Bonus Payments	Compensation Data
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Background Checks	
Criminal History	Criminal Records
Reference or Background Checks	
Employment Information	
Appeals Records Information	Benefits and Entitlements Data
Business Unit Division	Company Entity
Contract Type	Corporate Credit or Debit Card Numbers
Disciplinary Action	End Date
End Date and Reason for Termination	Exit Interview and Comments
Grade	Grievances and Complaints
Hours of Work	Job Application Details
Job Title Role	Line Reporting Manager
Military Status	Office Location

Performance Rating	Personnel Number
Previous Work History	Record of Absence/Time Tracking/Annual Leave
Salary	Start Date
Personal Identification	
Age	Date of Birth
Disability or Specific Condition	First Name
Full Name	Gender
Surname	Marital Status
Nationality	Signature
User Account Information	
User ID	
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages

Recipient of the personal data

Recipients of the data Internal Audit members, any person duly assigned by the Director of Internal Audit and the Principal Director Internal Audit and Professional Standards.

Internal audit reports are submitted to the President (or the RFPSS Supervisory Board) for decision on recommendations. The internal audit reports are forwarded to the management of the audited units and a copy is provided to the Board of Auditors.

As a general rule, the information presented in the internal audit reports shall be anonymised.

Purpose of sharing planning and conducting internal audits, following up on the implementation of recommendations

Transfer

Transfer No

Country where data might be transferred - Processor (Vendors) Microsoft - United States, Consulting Auditing Firms - Canada, Consulting Auditing Firms - United Kingdom, OpenText - United Kingdom

Transfer to public authority and/or International Organisation

Reasons for the transfer

Transfer mechanism(s)

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 26

Name Selection of members of SACEPO (Standing Advisory Committee before the EPO) and its working parties

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG5 - 52 - Legal Affairs

External processors

Microsoft

External processors	
Name Microsoft	

OpenText

External processors	
Name OpenText	

Any participant from outside the EEA

External processors	
Name Any participant from outside the EEA	

Microsoft

External processors

Name
Microsoft

Description of the processing

Description The SACEPO and its specialist SACEPO Working Parties (Quality, Rules, Guidelines, Patent Information and E-Patent Process) are composed of user representatives appointed by the President of the Office. Some of them are proposed by users associations, the remainder are directly identified and appointed by the Office.

The Sacepo secretariat collects the information provided by the IP stakeholders/associations and/or by the candidates themselves. It prepares the file for the final part of the deliberation and decision-making process. This involves a first evaluation of the suitability of the candidates also with regard to the need to have a sufficiently balanced composition of SACEPO and each of its working parties. This is related to the purpose of having a balanced representativeness of the users community (e.g. technical fields, SMEs versus big companies) and of the society (e.g. genders, nationality).

The candidates finally appointed by the President are informed via an official letter. Previous members who are not re-appointed are informed via email. Other unsuccessful candidates are informed indirectly, as the list of newly appointed SACEPO members is published on the SACEPO webpages of the EPO's Internet. The SACEPO webpages can be found here. https://www.epo.org/about-us/services-and-activities/Consultingourusers/sacepo/members.html

SACEPO secretariat stores the electronic information received via email in its dedicated SACEPO mailbox. Paper files might also be prepared, in which case they are stored in the archive room(s) of the SACEPO secretariat.

The personal data of all the successful and unsuccessful candidates is kept by the SACEPO Secretariat at least until the next selection round is over.

We process the following categories of personal data
- identification and contact details (mainly name, phone number, email address and nationality)
- information related to the candidate's professional background (mainly from the candidate's CV including education, employment history, professional memberships and current job title)
- information pertaining to the selection process (mainly related to EPO employees' input to the deliberation and decision-making process)
- any other information provided in the course of exchanges
- Case Management System ticket information (e.g. case number)
- in the case of newly appointed and re-appointed SACEPO members, identification details and information related to their professional background are published online on the SACEPO and EPO web pages (i.e. form of address, first name, last name, the user association they represent or mention of ad personam appointment, their employer's name and their current job title or position held).

Purpose of Processing Use the data of appointed members for the organisation of the SACEPO meetings, - Selection of members of SACEPO and its specialist SACEPO Working Parties, in such a way that the user groups are as representative as possible of the stakeholder groups which the Office would like to consult and of society as a whole. - publication of the appointments. - providing the SACEPO secretariat with a pool of potential candidates for next selection rounds.

Data Retention Personal data processed are stored for the period of time necessary to achieve the purpose for which they have been processed.

Personal data will be deleted/retained on the following basis:
- Personal data processed during the selection process are kept for as long as the data subjects are members of the SACEPO or its working parties.
- Personal data of former members or candidates not appointed serve as a pool of potential candidates and are deleted four years after the last completed selection process.
- The list of SACEPO member appointments will remain on the internet until the next round of appointments is published.
- Names and basic identification information of all SACEPO members are kept by the EPO for historical reasons.

Data subjects and categories of personal data

Externals

General	
User association	
Matter/Log file	
Attachments	Metadata
Contact Information	
Contact Details	Personal Email
Phone Numbers	Working email address
Professional Experience & Affiliations	
Affiliation	CV
Professional Memberships	Qualifications Certifications
Correspondence	
Additional Information which might be provided in the course of exchanges	
Employment Information	
Business Unit Division	Company Entity
Job Title Role	Office Location
Previous Work History	
Personal Identification	
First Name	Full Name
Gender	Surname

Nationality	
Education & Skills	
Education and Training History	Educational Degrees
Languages	

Employees

General	
Input provided during the deliberation and decision-making process	
Matter/Log file	
Attachments	Metadata
Contact Information	
Contact Details	Phone Numbers
Employment Information	
Business Unit Division	Department name and/or number
Job Title Role	Office Location
Personnel Number	Room Number
Personal Identification	
First Name	Surname

Recipient of the personal data

Recipients of the data (1) EPO hierarchy

(2) Other EPO employees (not hierarchy)

(3) Internal stakeholders of SACEPO

(4) The public

Purpose of sharing (1) EPO hierarchy involved in the internal deliberation and decision-making process.

(2) Office's employees involved in the selection process (on a need-to-know basis).

(3) Internal stakeholders of SACEPO might be consulted, in which case only the part of the personal data of the candidates necessary for this consultation is shared (usually name/contact details and specific criteria discussed)

(4) The public, as the list of newly appointed or re-appointed SACEPO members is published on the SACEPO webpages of the EPO's Internet

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Country where data might be transferred - Processor (Vendors) Microsoft - United States, OpenText - United Kingdom

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, International cooperation activities

Transfer mechanism(s) The recipient provided appropriate safeguards, Derogation in accordance with Art. 10 DPR

Derogations Art. 10 DPR The transfer is necessary for the performance of a task in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning, or to perform obligations arising from its duty of co-operation with the contracting states

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 39

Name Delivery of Patent Knowledge related data

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 46 - CIO / BIT, DG4 - 44 - General Administration, DG4 - 45 - CTO / BIT

Entity Name - Controller (Entities) DG5 - 54 - Patent Intelligence

External processors

Okta Inc

External processors	
Name Okta Inc	

ServiceNow

External processors	
Name ServiceNow	

Microsoft

External processors	
Name Microsoft	

Google Ireland Limited

External processors

Name
Google Ireland Limited

Google Ireland Limited

External processors
Name
Google Ireland Limited

Okta Inc

External processors
Name
Okta Inc

Microsoft

External processors
Name
Microsoft

ServiceNow

External processors
Name
ServiceNow

Description of the processing

Description The European Patent Office (EPO) distributes European Patent Grant procedure related data and world-wide patent data which can be downloaded by users from the EPO platform providing the service. Some of the data require user subscription and registration.

The datasets covered by this process include the bulk datasets listed here:
https://www.epo.org/en/searching-for-patents/data/bulk-data-sets .

Subscriber and subscription information is processed by the EPO's Customer Support Team (CSC) within the EPO and subscriber data corresponding to the data subscriptions are sent to the data hosting provider (an external service company) or to an internally managed platform. This subscription information processing is described in the scope of the record “Patent Knowledge Web Shop”.

Based on the users’ information, the hosting provider manages access to the data. EPO staff may also access and manage the user data.

Personal data is used during the processes of preparing the data, data delivery to users, analytics, and to provide support and distribute event information to users.

In special cases delivery may involve the use of post services. In these cases the data is prepared by PD Patent Knowledge and passed to PD General Administration for dispatch.

Data Retention User data is retained for up to 10 years (due to financial record retention policy as most of subscriptions require payment) after it can be reasonably expected that there is no immediate operational need anymore (e.g. cancellation of a subscription).

Technical service access data can be retained for up to 7 years in order to analyse usage patterns.

Information contained in the patent records is public data which is never deleted.

Purpose of Processing Delivery of data to users., Distribute information about products., Distribute support and event information to users., Analytics and service delivery, User access control.

Data subjects and categories of personal data

Externals

Network/application Interaction Data	
Session content	Session details
Session metadata	
Contact Information	
Contact Details	Home Address
Personal Email	Phone Numbers
Working email address	
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications

Employment Information	
Company Entity	Office Location
Browsing Information	
Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
Cookie Information	IP Address
Network Interaction History	URL
Website History	
Personal Identification	
First Name	Full Name
Gender	Surname
User Account Information	
Account Password	User ID

Employees

Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications
Browsing Information	
Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
Cookie Information	IP Address
Network Interaction History	URL
Website History	
User Account Information	
Password	User ID

Former Employees

Patent Process Related Data

Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications

Recipient of the personal data

Recipients of the data The patent record content can be made available to anyone who uses the service. These users may be world wide.

If necessary to perform their tasks, non-patent personal data may be shared on a need-to-know basis with staff undertaking duties in the following areas of the EPO and external contractors: Patent Knowledge, Finance, BIT, DG1, PD General Administration, PD European and International Affairs, PD 0.3 and senior EPO management (VP5 Office, MAC, President's Office).

Purpose of sharing

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation Published patent data are made available to the public world-wide.

Transfer mechanism(s) The recipient provided appropriate safeguards, Derogation in accordance with Art. 10 DPR

Country where data might be transferred - Processor (Vendors) Okta Inc - Costa Rica, Okta Inc - United States, Microsoft - United States, ServiceNow - Netherlands, Google Ireland Limited - Hong Kong, Google Ireland Limited - Taiwan, Google Ireland Limited - Brazil, Google Ireland Limited - Qatar, Google Ireland Limited - Indonesia, Google Ireland Limited - Singapore, Google Ireland Limited - Malaysia, Google Ireland Limited - Saudi Arabia, Google Ireland Limited - United States, Google Ireland Limited - Philippines, Google Ireland Limited - India, Google Ireland Limited - Australia, Google Ireland Limited - Chile

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, Protection against malware, login to Azure Active Directory, error analysis, load balancing, diagnostics data and connected experiences, Provision of services and technical support, The service is intended to deliver patent data to world-wide users.

Derogations Art. 10 DPR The transfer is made from a register which, according to the legal provisions of the European Patent Organisation, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down for such consultation are fulfilled in the particular case, The transfer is necessary for the performance of a task in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning, or to perform obligations arising from its duty of co-operation with the contracting states

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 40

Name Patent Knowledge News

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 46 - CIO / BIT, DG4 - 45 - CTO / BIT

Entity Name - Controller (Entities) DG5 - 54 - Patent Intelligence

External processors

Microsoft

External processors	
Name Microsoft	

Microsoft

External processors	
Name Microsoft	

Description of the processing

Description The EPO provides news content by various authors for inclusion in the patent knowledge on-line news (PKN) service as part of the EPO web site.

External and internal users access PKN via the standard EPO web site protocols and interact with the PKN service via a functional email account for the EPO's Patent Knowledge News, which is setup in order to:

- Facilitate communication between the EPO staff in charge of Patent Knowledge News and the users/readers/contributors.

- Facilitate information exchange (receiving questions, comments, suggestions, quiz results, enquiries and providing feedback) and other user engagement activities.

The EPO will answer the readers' questions directly or forward the inquiries to internal and/or external experts who would then respond to the reader.

To carry out the tasks and activities described, the Office uses Microsoft Office 365 applications.

Data Retention The retention policy is set to maximum 7 years. If considered appropriate, it is also deleted if it can reasonably be expected that there is no operational need anymore.

Microsoft Outlook retains personal data as long as it is necessary for the purposes for which personal data was collected. After expiration or termination of the Contract, Microsoft stores personal data for 90 days to allow the EPO to extract the data. After the 90-day retention period ends, Microsoft will disable EPO's account and delete the personal data within an additional 90 days, unless Microsoft is permitted or required by applicable law to retain such data.

Purpose of Processing Provide online access to Patent Knowledge News, Facilitate information exchange (receiving questions, comments, suggestions, enquiries and providing feedback) and other user engagement activities., Facilitate communication between the EPO staff in charge of Patent Knowledge News and the users/readers/contributors.

Data subjects and categories of personal data

Employees

Contact Information	
Contact Details	Home Address
Personal Email	Phone Numbers

Externals

Contact Information	
Contact Details	Personal Email
Phone Numbers	
Correspondence	
Personal information provided voluntarily	

Recipient of the personal data

Recipients of the data The personal data are disclosed on a need-to-know basis to the EPO staff involved in Patent Knowledge News related activities.

Personal data might be disclosed to Microsoft for maintenance, support and security purposes, as well as BIT and Microsoft staff involved in the data processing necessary to provide the Microsoft services.

Personal data will be shared with authorised persons responsible for the corresponding processing operation. They will not be used for any other purposes or disclosed to any other recipients.

Purpose of sharing - EPO staff: deliver service to the user by management and publication of Patent Knowledge News.
- Microsoft and BIT: provide the Microsoft services, as well as for maintenance, support and security purposes.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) Data Protection EU Comm Standard Contractual Clauses

Country where data might be transferred - Processor (Vendors) Microsoft - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, Security purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 41

Name European Publication Server

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 46 - CIO / BIT, DG4 - 45 - CTO / BIT

Entity Name - Controller (Entities) DG5 - 54 - Patent Intelligence

External processors

Google | European Union | Technology

External processors	
Name Google | European Union | Technology	

N.A.

External processors	
Name N.A.	

Description of the processing

Description The European Patent Office (EPO) publishes patent documents by decision of the President of the EPO published in the EPO Official Journal of February 2005, and the European Publication Server has been the sole legally authoritative publication medium for European A and B documents since 1 April 2005. All documents are available for public access from any location free of charge on their day of publication.

Patent publication data is prepared during the Patent Grant procedure, and subsequently distributed via the European Publication Server.

In addition to the above mentioned “content” processing, additional processing is undertaken in order to provide service usage analytics and ensure correct service functioning.

Purpose of Processing Analytics, and ensuring correct service functioning., Online distribution of published European Patent documents.

Data Retention The EP publications are public data, and therefore the data is not deleted.
User data is retained for up to 7 years after it can be reasonably expected that there is no immediate operational need anymore.

Data subjects and categories of personal data

Employees

Network/application Interaction Data	
Session content	Session details
Session metadata	
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications
Browsing Information	
Browser type	Browsing Time
Cookie Information	IP Address
Network Interaction History	Website History

Externals

Network/application Interaction Data	
Session content	Session details
Session metadata	
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications
Browsing Information	
Browser type	Browsing Time
Cookie Information	IP Address
Network Interaction History	Website History

Former Employees

Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications

Recipient of the personal data

Recipients of the data The patent record content can be made available to anyone who uses the service. These users may be world wide.

Where necessary to perform its tasks, non-patent personal data may be shared on a need-to-know basis with staff undertaking duties in the following areas of the EPO and external contractors: Patent Intelligence, BIT, DG1 and senior EPO management (VP5 Office, President Office, Corporate Governance Service (CGS), MAC), external contractors working for the aforementioned areas of the EPO may also have access.

Purpose of sharing Publication is done in accordance with the provisions of the European Patent Convention.
Administrative and operational information is shared to ensure correct functioning of the service and to facilitate usage analysis.

Transfer

Transfer No

Transfer to public authority and/or International Organisation The published data are publicly accessible.

Transfer mechanism(s) Derogation in accordance with Art. 10 DPR

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer The patent record content is made available to anyone world-wide., Publication is done in accordance with the provisions of the European Patent Convention.

Derogations Art. 10 DPR The transfer is made from a register which, according to the legal provisions of the European Patent Organisation, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down for such consultation are fulfilled in the particular case

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 42

Name PISE Services

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 45 - CTO / BIT, DG4 - 46 - CIO / BIT

Entity Name - Controller (Entities) DG5 - 54 - Patent Intelligence

External processors

Luminess

External processors	
Name Luminess	

Luminess

External processors	
Name Luminess	

Description of the processing

Description The European Patent Office (EPO) provides Patent Information Services for Experts (PISE) to users. Prior to dissemination, the content including data needs to be processed so that it is in the form ready to be disseminated.

These services include:
- EP FULL-TEXT to search European patent applications (A documents) and granted patents (B documents) and monitor new publications as they appear.
- EP BULLETIN SEARCH which gives access to information on the bibliographic and procedural status of European applications and patents from 1978 to the present.
- GLOBAL PATENT INDEX (GPI) to perform detailed searches in the EPO's worldwide bibliographic, legal event and full-text data sets.
- PATSTAT which contains bibliographical and legal event patent data from leading industrialised and developing countries.

These are web-based services, and some areas require user registration which is linked to an integrated Internet Access Control based upon the user credentials.

The patent procedure records may also contain personal information as an intrinsic part of the subject matter treated in the record (inventors, applicants, EPO officers etc).

In addition to the above mentioned “content” processing, additional processing is undertaken in order to provide service usage analytics and ensure correct service functioning.

Data Retention User data are kept for up to 7 years or earlier where it can be reasonably expected that there is no immediate operational need anymore (e.g. cancellation of a subscription).
Technical service access data are kept for up to 7 years for analysis purposes. Information contained in the patent records is public data which is never deleted.

Purpose of Processing Delivery of PISE services to users., Analytics and service delivery

Data subjects and categories of personal data

Externals

Network/application Interaction Data	
Session content	Session details
Session metadata	
Contact Information	
Contact Details	Country
Personal Email	Working email address
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications
Employment Information	
Company Entity	
Browsing Information	

Browser type	Browsing Time
Cookie Information	IP Address
Network Interaction History	Website History
Personal Identification	
First Name	Full Name
Gender	Surname
User Account Information	
Account Password	User ID

Employees

Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications

Former Employees

Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications

Recipient of the personal data

Recipients of the data The patent record content can be made available to anyone who uses the service. These users may be located world-wide.
Personal data of users may be shared with authorised persons responsible for the corresponding processing operations and any other EPO staff members who need to have access to the data only on a need to know basis.

Purpose of sharing

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation The patent related content is made available to anyone world-wide.

Transfer mechanism(s) Derogation in accordance with Art. 10 DPR

Country where data might be transferred - Processor (Vendors)
Luminess - France

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, The patent related content is made available to anyone world-wide.

Derogations Art. 10 DPR The transfer is necessary for the performance of a task in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning, or to perform obligations arising from its duty of co-operation with the contracting states

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network	

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 43

Name EPO hosted PK services

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 45 - CTO / BIT, DG4 - 46 - CIO / BIT

Entity Name - Controller (Entities) DG5 - 54 - Patent Intelligence

External processors

Okta Inc

External processors	
Name Okta Inc	

Google | European Patent Office | Technology

External processors	
Name Google | European Patent Office | Technology	

Google Ireland Limited

External processors	
Name Google Ireland Limited	

Not Applicable.

External processors

Name
Not Applicable.

Microsoft

External processors
Name
Microsoft

Description of the processing

Description The European Patent Office (EPO) provides external access to a restricted set of users for a Technology Intelligence Platform (TIP).

The Technology Intelligence Platform is EPO's next generation tool for external users with the purposes of:
- processing, analysing and visualising patent data;
- extracting patent information and patent knowledge from data;
- fostering collaboration within the patent information and knowledge community.

This platform comprises access to a range of EPO hosted patent electronic data collections and further allows for users to execute their own computer code to manipulate the data. Users may load additional data into the environment in accordance with the terms and conditions of the service and include it in their data processing. Access to the user data area is restricted to the specific user that uploads the data and to the EPO.

The use of the service and the data uploaded by users is strictly limited to the analysis of patent data in combination with relevant additional data sets in accordance with the terms and conditions of the service which are linked from the service web site. The processing steps implemented by the Technology Intelligence Platform include:

- Providing a user customised development environment (achieved through assigning user role(s)) and hosting associated data.
- Providing support, training, and promotion of EPO activities
- Proper maintenance and functioning of the platform
- Ensuring secure operations
- User access control and activity logging

Personal details of platform users are also used for ensuring acceptable use and functioning of the service.

Data Retention User data is retained for up to 7 years after it can be reasonably expected that there is no immediate operational need anymore (e.g. cancellation of a subscription).
Technical service access data can be retained for up to 7 years in order to analyse usage patterns.

Information contained in the patent records is public data which is never deleted.

Purpose of Processing Provide user access to the service., Providing support, training, and promotion of EPO activities, Ensuring compliance with the terms and conditions of use of the service., User activity logging., Usage analytics and ensuring correct and secure service functioning

Data subjects and categories of personal data

Externals

General

Any other information that complies with the terms and conditions of the service	
Network/application Interaction Data	
Session content	Session details
Session metadata	
Ticketing	
Ticket related data	
Contact Information	
Personal Email	Working email address
Correspondence	
Additional Information which might be provided in the course of exchanges	Personal information provided voluntarily
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications
Employment Information	
Company Entity	Language preference (of communication)
Browsing Information	
Browser type	Browsing Time
Cookie Information	IP Address
Network Interaction History	Search query
Website History	
Personal Identification	
First Name	Full Name
Gender	Surname
User Account Information	
Account Password	User ID

Employees

Patent Process Related Data

Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications
Browsing Information	
Browser type	Browser User Agent
Browsing Time	Cookie Information
IP Address	Network Interaction History
Search query	Website History
User Account Information	
Password	User ID

Recipient of the personal data

Recipients of the data Where necessary to perform their tasks, data may be shared on a need-to-know basis with staff undertaking duties in the following areas of the EPO: Patent Intelligence, BIT, DG1 and senior EPO management (VP5 Office, President Office, CGS, MAC, PD Communication,).

Personal data may be disclosed to third-party service providers for the provision of the services as well as maintenance and support purposes.

Access to the user data area is additionally available to the specific user that uploads the data.

Purpose of sharing

Transfer

Transfer No

Transfer to public authority and/or International Organisation The published patent data are publicly accessible world-wide.

Transfer mechanism(s) Derogation in accordance with Art. 10 DPR

Country where data might be transferred - Processor (Vendors) Google Ireland Limited - Hong Kong, Google Ireland Limited - Taiwan, Google Ireland Limited - Brazil, Google Ireland Limited - Qatar, Google Ireland Limited - Indonesia, Google Ireland Limited - Singapore, Google Ireland Limited - Malaysia, Google Ireland Limited - Saudi Arabia, Google Ireland Limited - United States, Google Ireland Limited - Philippines, Google Ireland Limited - India, Google Ireland Limited - Australia, Google Ireland Limited - Chile, Microsoft - United States, Okta Inc - Costa Rica, Okta Inc - United States

Reasons for the transfer The patent related content is intended to be made available to anyone world-wide.

Derogations Art. 10 DPR The transfer is made from a register which, according to the legal provisions of the European Patent Organisation, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down for such consultation are fulfilled in the particular case

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 45

Name Patent Knowledge Web Shop

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 41 - Finance, DG4 - 45 - CTO / BIT, DG4 - 44 - General Administration, DG4 - 46 - CIO / BIT

Entity Name - Controller (Entities) DG5 - 54 - Patent Intelligence

External processors

Ingenico | European Patent Office | Unknown

External processors	
Name Ingenico | European Patent Office | Unknown	

ServiceNow

External processors	
Name ServiceNow	

SAP

External processors	
Name SAP	

Commerzbank | European Patent Office | Unknown

External processors

Name
Commerzbank | European Patent Office | Unknown

Microsoft

External processors
Name
Microsoft

Worldline | European Patent Office | Unknown

External processors
Name
Worldline | European Patent Office | Unknown

Commerzbank

External processors
Name
Commerzbank

Description of the processing

Description The EPO online shop is an web based platform where individuals can order EPO Patent Knowledge related products and services where Patent Knowledge is understood to be knowledge that serves to foster the effective use and dissemination of patent data.

Personal data are processed and used as described below:

• Personal data is collected and processed for the purpose of processing orders and promotion and marketing activities of the EPO.

• The personal data of EPO online shop customers is collected during user account registration process. Customers connect to the EPO online shop area of the EPO website to register and/or maintain their account information. An account is required before using the EPO online shop to place orders.

• The personal data is stored in the back-end system of the EPO online shop and the EPO's SAP back-end system. The list of Patent Knowledge related products and services is dynamic, and the current status can be found in the EPO website. In certain cases, information in the back-end system may be manually entered by EPO Patent Knowledge staff.

• When needed to handle order processing related issues, personal data are used for identifying the user. To resolve the issue, further personal data provided by the user, might be used.

• To carry out promotion and marketing of EPO products and services. The users may be contacted via the communication channel indicated during the registration process.

• To carry out payment transaction processing for invoiceable products and services, necessary personal data are processed by the relevant EPO departments. The invoicing is undertaken by the Customer Service Centre (CSC) within the Patent Knowledge business area of the EPO, and is based on the information mentioned above. Payment processing in undertaken by the Finance department of the EPO and external contractors depending on the payment method.

• For IT support and maintenance, product and service delivery, improvement of the overall service and user experience.

Users may terminate subscriptions by contacting the EPO in accordance with the terms for the relevant products and services, and information will be retained in accordance with this record.

The tools and platforms are integrated across a range of domains, and encompass activities and products / services offered falling under the responsibilities multiple internal and external processors as further elaborated in this record.

Data Retention User data is retained for maximum 7 years from the time that a subscription ceases to be active. Information is retained whilst accounts are active. If considered appropriate, data is deleted if it can reasonably be expected that there is no operational need anymore.

Financial data is retained for 10 years, in line with the EPO financial regulations.

Purpose of Processing Provide a Webshop frontend for users, order processing, invoicing, user account registration and subscription management., IT support, delivery and maintenance., Service improvement., Payment transaction processing., Ad-hoc contact with users and marketing.

Data subjects and categories of personal data

Externals

General

Any other information	
Contact Information	
Contact Details	Country
Home Address	Personal Email
Phone Numbers	Working email address
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Financial	
Bank Account Information	Bank Account Number
Credit Card Number	Debit Card Number
VAT ID Number	
Employment Information	
Company Entity	
Browsing Information	
Browsing Time	Cookie Information
IP Address	Network Interaction History
Website History	
Personal Identification	
First Name	Full Name
Gender	Surname
Nationality	Signature
Education & Skills	
Languages	
User Account Information	
Account Age	Account Number
Account Password	

Recipient of the personal data

Recipients of the data The patent record content can be made available to Webshop customer ordering a relevant product. These customers may be world wide.

Where necessary to perform its tasks, non-patent personal data may be shared on a need-to-know basis with staff undertaking duties in the following areas of the EPO: Patent Intelligence, BIT, Finance, senior EPO management (Observatory on Patents and Technology, VP1 Office, VP4 Office, VP5 Office, President's Office, CGS, MAC) as well as with external contractors providing related processing.

Purpose of sharing

Transfer

Transfer No

Country where data might be transferred - Processor (Vendors)
Microsoft - United States, SAP - Germany

Transfer to public authority and/or International Organisation

Reasons for the transfer

Transfer mechanism(s)

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 46

Name PK User Support

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 47 - Procurement and Vendor Management, DG4 - 41 - Finance, DG4 - 45 - CTO / BIT, DG4 - 46 - CIO / BIT

Entity Name - Controller (Entities) DG5 - 54 - Patent Intelligence

External processors

ServiceNow

External processors	
Name ServiceNow	

Microsoft

External processors	
Name Microsoft	

Microsoft

External processors	
Name Microsoft	

Description of the processing

Description The EPO recognises the importance of high-quality research on patent-related intellectual property (IP) matters to inform policymakers and facilitate sound business decisions in a context where intangible assets, innovation and IP rights have become pivotal in the economy. With the EPO Academic Research Programme (EPO ARP), launched in 2017, we seek in particular to encourage more academic IP research and to promote the dissemination of research results.

In order to facilitate effective research collaboration, we support collaborative research schemes in which scientific partner institutions team up to work on projects with a broader scope, bigger budget and longer duration, and with the potential to involve a range of EPO departments.

This process relates to EPO activities undertaken in the Administration of the EPO ARP related tasks, and these include:

- Organising acalls for EPO ARP research proposals
- Overall EPO ARP programme administration including financial aspects
- Processing and evaluation of EPO ARP research proposals
- Administering contacts and information exchange with EPO ARP participants and related parties
- Evaluating EPO ARP results
- Surveys, questionnaires, discussion fora, workshops, etc which may all be undertaken either on.line or in person.

Data Retention User data is retained for up to 7 years after it can be reasonably expected that there is no immediate operational need anymore.

Purpose of Processing - Organising acalls for EPO ARP research proposals - Overall EPO ARP programme administration including financial aspects - Processing and evaluation of EPO ARP research proposals - Administering contacts and information exchange with EPO ARP participants and related parties - Evaluating EPO ARP results - Surveys, questionnaires, discussion fora, workshops, etc which may all be undertaken either on.line or in person.

Data subjects and categories of personal data

Externals

General	
Answers to surveys, assessments or quizzes	Attendees' lists
Multimedia material	
Social	
Social Media Account	
Sensory and Electronic Information	
Audio Information	Electronic Information
Visual Information	
Contact Information	
Contact Details	Country
Phone Numbers	Working email address
Professional Experience & Affiliations	

Affiliation	CV
Entry or deletion date as member of an association	Professional Memberships
Qualifications Certifications	
Correspondence	
Additional Information which might be provided in the course of exchanges	Feedback received
Personal information provided voluntarily	
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of a patent (claims, description, drawings, abstract)
Personal data potentially included within the content of patent procedure related information and publications	
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Employment Information	
Business Unit Division	Company Entity
Department name and/or number	Duration of employment
Job Title Role	Office Location
Previous Work History	
Browsing Information	
Browsing Date and Time	IP Address
Network Interaction History	
Personal Identification	
Date of Birth	Digital signature
First Name	Full Name
Gender	Surname
Nationality	Picture
Signature	

Education & Skills	
Education and Training History	Languages
Technical expertise	

Recipient of the personal data

Recipients of the data The patent record content can be made available to anyone who uses the service. These users may be world wide.

Where necessary to perform its tasks, non-patent personal data may be shared on a need-to-know basis with staff undertaking duties in the other areas of the EPO and in particular: Patent Intelligence, BIT, DG1, EPO Observatory, Chief Sustainability Office, PD Communication, Chief Economist Office, and senior EPO management (President Office, VP5 Office, VP4 Office, MAC).

Information may also be shared with external contractors engaged by the above mentioned EPO units.

Purpose of sharing

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards, Data Protection EU Comm Standard Contractual Clauses

Country where data might be transferred - Processor (Vendors)
Microsoft - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 47

Name PATLIB

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 46 - CIO / BIT, DG4 - 45 - CTO / BIT

Entity Name - Controller (Entities) DG5 - 54 - Patent Intelligence

External processors

SAP

External processors	
Name SAP	

Microsoft

External processors	
Name Microsoft	

Poppulo

External processors	
Name Poppulo	

Microsoft

External processors

Name
Microsoft

Description of the processing

Description The "PATLIB centres", standing for PATent LIBrary, provide local access to patent information and related issues. They are familiar with the local industrial, economic and business landscape, and provide valuable services to entrepreneurs, SMEs, private inventors and students.

The EPO co-ordinates the PATLIB network.

Personal data are processed only for the purpose of carrying out the administration, collaboration and communication involving the PATLIB centres and partners.

PATLIB related processing:

- communicating within the PATLIB network and partners
- keeping an online directory of PATLIB centres and experts. The directory, which is available to the public, can be used to find IP-specific support and contains contact details of the PATLIB centres and their experts. The centres themselves decide on the type and amount of disclosed details
- collaborating with PATLIB network staff
- collaborating with third parties
- administering the PATLIB network
- PATLIB Committee related activities
- ad-hoc PATLIB related meetings
- PATLIB News related activities
- identifying participants and contributors to PATLIB activities
- organising PATLIB and other IP-related EPO meetings, events and training courses
- organising the participation of data subjects with certain recorded skills within the PATLIB network as experts, speakers, consultants etc.
- organising the participation of data subjects and their contributions to other EPO-led activities where input from PATLIB centres is likely to be beneficial
- organising the participation of data subjects in third-party activities commissioned and/or authorised by the EPO
- keeping records of data subjects' participation in activities organised within the PATLIB network or by the EPO, and of the business cases submitted and any feedback received
- documenting exchanges within the PATLIB network
- exchanging information on events on the PATLIB network events calendar
- self-assessments from PATLIB centres
- annual reports from PATLIB centres
- creating and distributing video and sound recordings of data subjects for the purpose of promoting knowledge-sharing in the area of IP and patent-related matters.

Data Retention Personal data will be kept for as long as the person is a member of the network or is a collaboration partner and three years thereafter.

Purpose of Processing Administration of PATLIB network, Organising PATLIB and other IP-related EPO meetings, events and training courses, Annual reports from PATLIB centres, Inviting data subjects with certain recorded skills to collaborate within the PATLIB network as experts, speakers, consultants, etc., Document exchange within the PATLIB network, Providing data subjects with information about the PATLIB activities by means of a regular email, Keeping a record of data subjects' participation in activities organised in the PATLIB network, the business cases submitted and any feedback received., creating and distributing video and sound recordings of data subjects for the purpose of promoting knowledge-sharing in the area of IP and patent-related matters., Self-assessments from PATLIB centres, Providing data subjects with invitations to PATLIB and other IP-related EPO meetings, events and trainings, Email Communication and User Questionnaire Management, Identifying participants and contributors to PATLIB activities, Information exchange on events within the PATLIB network events calendar, Communicating and records of communication within the PATLIB network and with partners, Ad-hoc PATLIB related meetings, PATLIB Committee related activities, PATLIB News related activities, Keeping an online directory of PATLIB centres and experts; the directory is available to the public to find IP specific support and contains contact details of the PATLIB centres and their experts. Through to self-administration, the centres decide on type and amount of disclosed details, Collaborating with PATLIB network staff and third parties

Data subjects and categories of personal data

Externals

Social

Social Media Account	Social Media Contact
Sensory and Electronic Information	
Audio Information	Visual Information
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Employment Information	
Business Unit Division	Company Entity
Contract Type	Corporate Credit or Debit Card Numbers
End Date	Hours of Work
Job Title Role	Office Location
Previous Work History	
Personal Identification	
Age	Date of Birth
Disability or Specific Condition	First Name
Full Name	Gender
Surname	Nationality
Signature	
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
General	
Answers to surveys, assessments or quizzes	
Health Data	
Health Data	
Contact Information	
Contact Details	Emergency Contact Details
Home Address	Personal Email

Phone Numbers	Working email address
Professional Experience & Affiliations	
Professional Memberships	Qualifications Certifications
Financial	
Bank Account Information	Bank Account Number
Credit Card Number	Debit Card Number
Insurance Information	
Browsing Information	
Browsing Time	Cookie Information
IP Address	Network Interaction History
Website History	
User Account Information	
Account Age	Account Number
Account Password	
Government Identifiers	
National Identity Card Details	Passport Number

Employees

Social	
Social Media Account	Social Media Contact
Social Media History	
Sensory and Electronic Information	
Audio Information	Visual Information
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Employment Information	
Business Unit Division	Line Reporting Manager
Office Location	Personnel Number

Personal Identification	
Age	Date of Birth
Disability or Specific Condition	First Name
Full Name	Gender
Surname	Nationality
Signature	
Education & Skills	
Education and Training History	Languages
Health Data	
Health Data	
Contact Information	
Contact Details	Emergency Contact Details
Personal Email	Phone Numbers
Working email address	
Professional Experience & Affiliations	
Professional Memberships	Qualifications Certifications
Financial	
Bank Account Information	Bank Account Number
Credit Card Number	Debit Card Number
Browsing Information	
Browsing Time	Cookie Information
IP Address	Network Interaction History
Website History	
User Account Information	
Account Age	Account Number
Account Password	Password
User ID	
Government Identifiers	

Passport Number	

Contractors

General	
Answers to surveys, assessments or quizzes	
Health Data	
Health Data	
Sensory and Electronic Information	
Audio Information	Visual Information
Contact Information	
Contact Details	Emergency Contact Details
Home Address	Personal Email
Phone Numbers	Previous Residence Address
Teleworking address	Working email address
Financial	
Bank Account Information	Bank Account Number
Credit Card Number	Debit Card Number
Routing Number	
Health Insurance Information	
Insurance Policy Information	Unique Identifier for Subscriber

Recipient of the personal data

Recipients of the data The personal data are disclosed on a need-to-know basis to the following recipients:
• Participants in the PATLIB network and activities
• Collaboration partners
• EPO staff members and non-EPO staff working on behalf of the EPO undertaking relevant duties
• Staff of national patent offices

The personal data are not disclosed to any other recipient.

Furthermore, the part of personal data disclosed in the online directory is available to the public without restriction.
The PATLIB Centre is responsible for the accuracy of its own data within the PATLIB directory.
Any third-party is directly responsible for misusing the publicly accessible data within the PATLIB directory.

Personal data might be disclosed to third-party service providers for maintenance and support purposes.

Personal data will only be shared with authorised persons responsible for the corresponding processing operations and are not used for any other purposes or disclosed to any other recipients.

Purpose of sharing

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation National Patent Offices

Transfer mechanism(s) The recipient provided appropriate safeguards, Derogation in accordance with Art. 10 DPR

Country where data might be transferred - Processor (Vendors) SAP - Germany, Microsoft - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, International cooperation activities, Public Authorities/Government Bodies, Further development of the PATLIB Network, To facilitate the execution of PATLIB related activities

Derogations Art. 10 DPR The transfer is necessary for the performance of a task in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning, or to perform obligations arising from its duty of co-operation with the contracting states

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 50

Name Off-site storage of PGP paper files

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG1 - 11 - COO

External processors

Iron Mountain Nederland B.V.

External processors	
Name Iron Mountain Nederland B.V.	

Iron Mountain (Deutschland) Service GmbH

External processors	
Name Iron Mountain (Deutschland) Service GmbH	

POT and Zoons B.V. Databankweg 18 Amersfoort The Netherlands

External processors	
Name POT and Zoons B.V. Databankweg 18 Amersfoort The Netherlands	

The stored paper is transported to and kept at a contractor's site which is in a member state of the EPC

External processors

Name	
The stored paper is transported to and kept at a contractor's site which is in a member state of the EPC	

Description of the processing

Description Paper originals submitted by users of the patent grant process of the EPO scanned on-site and kept on-site for a number of months in case scanning problems are detected. The original paper is stored in boxes.

After the initial on-site storage period the boxes are transported either from The Hague or Munich to the offsite storage contractor Iron Mountain either in Germany or The Netherlands. Here the boxes are stored in a secure warehouse. Upon request of the EPO (rare occurrence about 10 times per year) a document is requested to be retrieved from a box and to be sent back to the EPO either as original pape or as a scanned electronic version.

Paper files containing personal data stored at the Contractor premises are locked in a secure location with restricted access.

For personal data processed on systems hosted at the Contractor premises, the providers processing the personal data have committed in a binding agreement to comply with their data protection obligations under the applicable data protection legal frameworks. These systems are required to have implemented appropriate technical and organisational measures such as: physical security measures, access and storage control measures, securing data at rest (e.g. by encryption); user, transmission and input control measures (e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), audit logging); conveyance control measures (e.g. securing data in transit by encryption). The paper file boxes are stored in a secure warehouse and the external contractor has signed a contract, which includes clauses on technical conditions, security details and a confidentiality agreement.

In line with the retention times, the EPO initiates safe destruction of the boxes. They are retrieved from the storage warehouse and transported to a specialised destruction company which carried out secure destruction.

Data Retention Legal requirement is to keep the original paper submissions 5 years from the end of the year they were filed in.

Leaving one year safety margin the EPO has destroyed the scanned original paper older than 6 years.

However, any paper files earmarked for use for artistic and historical purposes will be kept in the EPO's cultural space for no longer than 60 years from the end of the year they were filed in.

Purpose of Processing Legal requirement Rule 147 EPC and PCT section 705bis

Data subjects and categories of personal data

Employees

Contact Information	
Phone Numbers	
Employment Information	
Business Unit Division	

Personal Identification	
First Name	Full Name
Surname	

Externals

Contact Information	
Contact Details	Home Address
Personal Email	Phone Numbers

Recipient of the personal data

Recipients of the data At contractor: staff of Iron Mountain Nederland B.V. and Iron Mountain (Deutschland) Service GmbH
At EPO: staff of directorate 152 interacts with the contractor

Purpose of sharing Legal requirement Rule 147 EPC and PCT section 705bis

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums)., no privacy and security and risk assessment carried out by the EPO, Authentication methods: The email address and password in combination with one of the two-factor authentication options provided by the EPO's Okta Customer Identity and Access Management (CIAM) system. o Google Authenticator: by entering the single-use code generated by this app o Okta Verify: by entering the single-use code generated by this app o Phone: by entering the single-use code sent to the phone via text message (SMS) or voice call o Email: by entering the single-use code sent to the email address associated with the EPO account

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 57

Name Tender procedures and agreements between external supplier and the EPO

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 41 - Finance

Entity Name - Controller (Entities) DG0 - 031 - Chief Business Analyst

External processors

Bidders / contractors

External processors	
Name Bidders / contractors	

Description of the processing

Description For most procurement procedures PD011 makes largely use of the administrative support of Central Procurement (CP), by participating to main phases and by approving the key proposed decisions (choice of procedure, choice of supplier, under art. 22a FinRegs and implementing rules), therefore the same description should apply as the one provided by CP to the DPO. The processing of personal data is necessary e.g. for:
- Registering the person/company applying for the tender (CP)
- for distribution and dissemination to the Award Committee (CP),
- to communicate with the person/company in the different phases of the tender processing (CP).
- To eventually invite the person/company to a meeting with the Award Committee to present their offer and answer questions.(CP)

Purpose of Processing Personal data is processed for the purpose of selecting a company to deliver product or services to the EPO following defined criteria and conditions and for accountability purposes

Data Retention Personal data will be kept by the EPO to following the legal obligations (directive on contract: Agreement No. 2016/3286 relating to the provision of consultancy services for surveys among patent applicants and first amending agreement No. 2017/3041) for keeping such category of data:
- the data is stored in FIPS and in physical original paper form in a closed room for accountability purposes for a maximum period of 12 years after the contract has been finalised behind lock in storage cabinets.
- contact details can be kept as part of a contact details database shared internally among EPO departments in order for them to contact data subjects for future tenders.

Data subjects and categories of personal data

Externals

Contact Information	
Contact Details	Working email address
Financial	
Bank Account Information	Bank Account Number
Personal Identification	
First Name	Full Name
Nationality	Signature

Employees

Contact Information	
Contact Details	

Recipient of the personal data

Recipients of the data Personal data depending on its type and the purposes of its processing is made accessible only on a need to know basis to EPO staff.

Different business units at the EPO will have access to the information stored on the contact details database on a need to know basis, e.g. in order for them to contact data subjects for future tenders.

Purpose of sharing Personal data depending on its type and the purposes of its processing is made accessible only on a need to know basis to EPO staff.

Different business units at the EPO will have access to the information stored on the contact details database on a need to know basis.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation No

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer Contact data of the EPO employee responsible for administrative matters is communicated to the bidders / contractors.

Transfer mechanism(s) Derogation in accordance with Art. 10 DPR

Derogations Art. 10 DPR The transfer is necessary for the performance of a task in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning, or to perform obligations arising from its duty of co-operation with the contracting states

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 64

Name List of contact names to support settlement and safekeeping of securities

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG5 - 5 - Legal and International Affairs

Entity Name - Controller (Entities) DG0 - 05 - Administration of Reserve Funds

Description of the processing

Description The Administration of the Reserve Funds has appointed multiple financial institutions to provide cash depository services (current accounts and term deposits) and one financial institution to provide cash depository and extended custody services including settlement and safekeeping of securities, including tax reclaim services and performance calculation services for assets owned by the European Patent Organisation.

All financial institutions have been selected for operational purposes, the personal data of its employees are stored in a EPO Database.

Data Retention The existing contact list is overwritten each time an update is received. Historic data is not stored or archived.

The overall retention period runs until the end of the contract with the service provider.

Purpose of Processing Personal data of the service providers' employees are processed for the purpose of the depository services as well as the general custody, settlement, tax reclaim, performance reporting and other services as outlined within the contractual framework on behalf of the European Patent Organisation.

Data subjects and categories of personal data

Externals

Contact Information	
Contact Details	Phone Numbers
Working email address	
Employment Information	
Business Unit Division	Company Entity

Job Title Role	Office Location
Personal Identification	
First Name	Surname

Recipient of the personal data

Recipients of the data The contact list obtained from BNP is made available within PD 05 on the document management platform.

The contact details for HVB , BLB and HSBC are only made available to the cash portfolio managers and their backups.

The safety measures for the Office apply, and access is only given to RFPSS staff.
A transfer of professional personal data to Legal Affairs in case of a litigation or legal dispute is possible.

Purpose of sharing A transfer of personal data to Legal Affairs in case of a litigation or legal dispute is possible.

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures All personal data related to the custodian bank employees are stored in secure IT applications according to the security standards of EPO. These include: • User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication; • Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum; • Logical security hardening of systems, equipment and network: 802.1x for network access, encryption of endpoint devices, AV on all devices; • Physical protection: EPO access controls, additional access controls to datacentre, policies to lock offices; • Transmission and input controls (e.g. audit logging, systems and network monitoring): security monitoring with Splunk; • Security incidence response: 24/7 monitoring for incidents, on-call security expert.

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 65

Name List of contact names to support dealing in financial securities and cash management

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG0 - 05 - Administration of Reserve Funds

Description of the processing

Description The Administration of the Reserve Funds makes use of various outside contractors (counterparties) for dealing in financial securities and cash management.
For operational purposes, contact details of these contractors is stored in an EPO Database.

Data Retention Contact details of data subjects (contact persons) are stored for operational purposes as long as the service provider (institution) is used for dealing in financial securities or cash management transactions.

Regular updates of the data are made when updates are being received or when contact persons change. Data records are amended or erased, and no historic records are maintained. At least once a year, during the annual review of the counterparties, the collected data is erased when the counterparty is no longer an active service provider.

Purpose of Processing Personal data is processed for the purpose of cash transactions., Personal data is processed for the purpose of dealing in securities.

Data subjects and categories of personal data

Employees

Contact Information	
Contact Details	
Correspondence	
Chat content	

Externals

Contact Information	
Contact Details	Phone Numbers
Working email address	
Personal Identification	
First Name	Surname

Recipient of the personal data

Recipients of the data Personal data is accessed for operational purposes by Fund Administration (PD 05) staff. In exceptional cases, personal data which is part of contracts might be shared with the EOP Legal Affairs department for legal due diligence purposes.

Purpose of sharing To ensure business continuity

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures All personal data related to contractors is stored in secure IT applications according to the security standards of EPO. These include: • User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication; • Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum; • Logical security hardening of systems, equipment and network: 802.1x for network access, encryption of endpoint devices, AV on all devices; • Physical protection: EPO access controls, additional access controls to datacentre, policies to lock offices; • Transmission and input controls (e.g. audit logging, systems and network monitoring): security monitoring with Splunk; • Security incidence response: 24/7 monitoring for incidents, on-call security expert.

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 66

Name List of contact names to support use of RFPSS investment management platform.

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG0 - 05 - Administration of Reserve Funds

Description of the processing

Description The Administration of the Reserve Funds has appointed an external contractor, SS&C Solutions Limited, London, England, for the managed services of our RFPSS investment management platform. This platform is the set of services, tools and software required to manage the RFPSS assets.
The platform also connects to financial data providers (e.g. Bloomberg, Nordea, MSCI, …) and is connected to the risk management tool (Barra).

For operational purposes, the professional personal contact details of SS&C employees, as well as those of the financial data providers and the risk management tool are stored in RFPSS files (= Outlook).

Data Retention The data is stored for the duration of the contract with the service provider.

Purpose of Processing Personal data of employees are processed for operational purposes, The personal data of SS&C London's employees are processed for operational purposes.

Data subjects and categories of personal data

Externals

Contact Information	
Contact Details	Phone Numbers
Working email address	
Employment Information	
Business Unit Division	Company Entity

Job Title Role	Office Location
Personal Identification	
First Name	Surname

Recipient of the personal data

Recipients of the data Personal data is accessed for operational purposes by Fund Administration (PD 0.5) staff. In exceptional cases, personal data which is part of contracts might be shared with the EPO Legal Affairs department for legal due diligence purposes.

Purpose of sharing Operational and/or legal due diligence purposes.

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures All personal data related to SS&C employees are stored in secure IT applications according to the security standards of EPO. These include: • User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication; • Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum; • Logical security hardening of systems, equipment and network: 802.1x for network access, encryption of endpoint devices, AV on all devices; • Physical protection: EPO access controls, additional access controls to datacentre, policies to lock offices; • Transmission and input controls (e.g. audit logging, systems and network monitoring): security monitoring with Splunk; • Security incidence response: 24/7 monitoring for incidents, on-call security expert.

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 68

Name Customer Services Management (CSM)

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 46 - CIO / BIT

Entity Name - Controller (Entities) DG1 - 15 - Customer Journey and KAM, DG1 - 1 - Patent Granting Process

External processors

ServiceNow

External processors	
Name ServiceNow	

ServiceNow Nederland B.V.

External processors	
Name ServiceNow Nederland B.V.	

ServiceNow

External processors	
Name ServiceNow	

Description of the processing

Description For EPO customer services management (CSM), a cloud-based software is applied allowing to receive, process and monitor incoming customer enquiries (received by phone, mail or contact form) and permitting integration with MS Teams.

At the EPO, when an enquiry is sent to support@epo.org or received either via the webform by contact@epo.org or by phone is received at the EPO,
the sender data are compared against the contact details in our database to identify the sender and allow their enquiry to be routed. This makes it possible to automatically acknowledge receipt of the enquiry, update and reply to the user and monitor any pending requests, in order to provide the best possible user experience.

The contact details are only needed, processed and stored in so far as they are required to handle user enquiries about EPO tools, pending applications for a European patent, international PCT applications, opposition and limitation/revocation files, patent information issues and EPO products and to handle user questions, payment-related queries and other issues which are linked to the mission and services provided by the EPO.

Personal data are processed in order to:

• respond to enquiries/questions/issues received as part of Customer Service Management
• gather information about categories of user or the types of issue users address (statistical purposes and trend monitoring)

The processing is not intended to be used for any automated decision-making, including profiling.

The personal data processed as part of Customer Service Management are stored in Germany, which is considered a country where an adequate level of protection of personal data is ensured. Stored personal data are not accessed from a country that does not ensure an adequate level of data protection. Specific safeguards, including a data processing agreement with the provider, have been put in place to mitigate the risks.

Personal data will not be transferred to recipients outside the EPO which are not covered by Article 8(1), (2) and (5) DPR unless an adequate level of protection is ensured. In the absence of an adequate level of protection, a transfer can only take place if appropriate safeguards have been put in place and enforceable data subject rights and effective legal remedies for data subjects are available, or if derogations for specific situations as per Article 10 DPR apply).

If the enquiries/questions/issues received relate to formal complaints or feedback, please refer to the data protection statement on the processing of personal data within the context of formal complaints and feedback:
https://link.epo.org/web/data_protection_statement_processing_personal_data_formal_complaints_and_feedback_en.pdf

Data Retention Personal data will be kept only for the time needed to achieve the purposes for which they are processed. They will be stored as long as processing is operational.
Contact details will be stored for five years after they were last used or updated, i.e. after the last interaction with the data subject as part of Customer Service Management.
Personal data received with an enquiry will be anonymised five years after the ticket was closed, so it can be used for statistical purposes.
In the event of a formal appeal/litigation, all data held at the time the formal appeal/litigation was initiated will be retained until the proceedings have been closed.

Purpose of Processing To handle incoming enquiries, to receive and to reply to a question/query/issue addressed to the EPO, ranging from questions on our filing services to procedural patent application-related queries.

Data subjects and categories of personal data

Externals

Phone Call Information	
Caller's Phone Number	Phone Call Date and/or Time
Ticketing	
Ticket related data	
Physical and/or Digital Identifiable Assets	
Smart Card Number	
Contact Information	
Contact Details	Home Address
Mobile Phone Number	Personal Email
Phone Numbers	Private Phone Number
Working email address	
Device Management Data	
Account ID	
Correspondence	
Personal information provided voluntarily	
Employment Information	
Business Unit Division	Company Entity
Department name and/or number	Job Title Role
Language preference (of communication)	Office Location
Personal Identification	
First Name	Full Name
Surname	

Employees

Ticketing	
Ticket related data	
Contact Information	
Contact Details	Personal Email

Phone Numbers	
Personal Identification	
First Name	Surname
User Account Information	
User ID	

Contractors

Ticketing	
Ticket related data	
Contact Information	
Phone Numbers	Working email address
Employment Information	
Office Location	
Personal Identification	
Full Name	
User Account Information	
User ID	

Recipient of the personal data

Recipients of the data Personal data are disclosed on a need-to-know basis to the EPO staff working in:

• DG 1: departments responsible for operations and quality management
• DG 4: Finance
• DG 5: Patent Law and the Legal Division

Personal data may be disclosed to third-party service providers for maintenance and support purposes.

Personal data will only be shared with authorised persons responsible for the necessary processing operations. They will not be used for any other purposes or disclosed to any other recipients.

Additionally, in line with the requirements set forth in Article 6, limited access to personal data may be granted on a need-to-know basis should this be deemed necessary and proportionate for a specific purpose to EPO staff working in other organisational unit(s) to perform tasks carried out in the exercise of their official activities, e.g. so staff in D432 can prepare anonymised reports/analyses. Such processing will take place on a case-by-case basis in accordance with the DPR requirements and the principles of confidentiality and accountability.

Purpose of sharing Personal data will only be shared with authorised persons responsible for the necessary processing operations. They will not be used for any other purposes or disclosed to any other recipients.

Additionally, in line with the requirements set forth in Article 6, limited access to personal data may be granted on a need-to-know basis should this be deemed necessary and proportionate for a specific purpose to EPO staff working in other organisational unit(s) to perform tasks carried out in the exercise of their official activities, e.g. so staff in D432 can prepare anonymised reports/analyses. Such processing will take place on a case-by-case basis in accordance with the DPR requirements and the principles of confidentiality and accountability.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards, Data Protection EU Comm Standard Contractual Clauses

Country where data might be transferred - Processor (Vendors) ServiceNow - Netherlands

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures For transfer of personal data, the provider uses a controlled access feature hopping (HOP) functionality. This is an extension of the production cloud environment and allows authorized employees ("users") to access and handle customer data, with the prior consent of the customer, in a controlled environment which maintains controls to restrict data from being exfiltrated. These functionalities reduce the probability that customer data and assets will be compromised. The provider also has appropriate internal regulations and policies that define exactly how data should be handled., All personal data processed in the systems hosted at the EPO premises are stored in secure IT applications according to the security standards of EPO. These include: - User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. - Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. - Logical security hardening of systems, equipment and network: 802.1x for network access, encryption of endpoint devices, AV on all devices. - Physical protection: EPO access controls, additional access controls to datacentre, policies to lock offices. - Transmission and input controls (e.g. audit logging, systems and network monitoring): security monitoring with Splunk. Security incidence response: 24/7 monitoring for incidents, on-call security expert' For personal data processed on Service Now systems, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: - Physical security measures. - Access control measures: role-based, principles of need-to-know and least privilege. - Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. - User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, antimalware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management. - Transmission control measures: audit logging, System and network monitoring. - Input control measures: audit logging, System monitoring. According to an internal security review and following the information from the ServiceNow Trust and Compliance Center, their operations cover all areas of ISO27001 and are in line with the EPO 'Cloud Computing Guidance Note v1.1'. According to this evaluation (which has been provided as evidence and proof for the contract with ServiceNow), the criteria of … - Service Availability/Disaster Recovery Confidentiality - Security and Integrity - Auditability - Cloud and Provider Location - Reversibility/Portability/Exit - Provider's Reliability and Solvency/Insurance - Certifications … have been successfully met. Provider's security framework is based on ISO/IEC 27002:2013. It has been an ISO 27001 certified organization since 2012 and is also ISO/IEC 27017:2015 and 27018:2019 certified. Provider also applies industry recognized information security frameworks. These include ISO/IEC 27001:2013, ISO/IEC 27017:2015, and 27018:2014, as well as accreditation with regional standards and regulations.

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 75

Name European Patent Register

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG1 - 1 - Patent Granting Process, DG5 - 54 - Patent Intelligence

Entity Name - Controller (Entities) DG5 - 53 - Patent Law and Procedures

External processors

ServiceNow

External processors	
Name ServiceNow	

Trustees outside Member States

External processors	
Name Trustees outside Member States	

Microsoft

External processors	
Name Microsoft	

Microsoft

External processors

Name
Microsoft

ServiceNow

External processors
Name
ServiceNow

Description of the processing

Description According to Article 20 EPC, the Legal Division (embedded in PD 5.2 legal affairs) shall be responsible for decisions in respect of entries in the Register of European Patents and it therefore administers the European Patent Register.
The Legal Division performs its duties in accordance with the Decision of the President of the European Patent Office dated 21 November 2013 concerning the responsibilities of the Legal Division.

The personal data necessary to perform the related processing operations (i.e. the information concerning documents pursuant to Rules 14 EPC, 22 EPC, 23 EPC, 24 EPC, 142 EPC or R142 EPC) is received mostly internally from a DG1 formalities officer via a Madras mailbox message in the legal division (in exceptional cases, the personal data can be received by fax or post), when guidance/legal advice is needed (Rule 22 EPC) or the procedural step (Rule 142 EPC) belongs to the responsibility of the legal division.

A member of the legal division makes an assessment and takes a decision on whether an update or a change on the register is necessary. In isolated cases the matter might necessitate legal advice (see corresponding record on legal advice). The registration of the decision is done in Madras.

The European Patent Register is being updated automatically following the registration. A communication informing the relevant party is usually sent by post by the legal division or, in case the representative has a dedicated Madras mailbox, the communication is notified automatically to him there. In some specific cases, the notification takes place via DG1 formalities officers (depending on the EPC Rule).

In case a request reaches the legal division via DG1 ticketing system: The ticketing system sends automatic emails to the mailbox of the legal division, those emails do however not entail any personal data, they only provide a ticket number and a link to access the ticketing system. The requester receives the answer via this ticketing system. In exceptional cases, when the requesters have further questions, they can contact directly the legal division via email. in such case corresponding personal data is shared via email.

All documents filed in the proceedings are stored in Madras.

The data subjects concerned are applicants, representatives, opponents, third parties and inventors pursuant to Rule 21 EPC.

Further personal data may be processed if sent by the parties, especially the information triggering the potential change of the register (e.g according to the Rule 22 EPC, the documents providing evidence of a transfers of an a European patent application). In some cases, such personal data is of sensitive nature (e.g., medical reports). Possibly personal data related to health in cases regarding Rule 142(1)(a) EPC.

Purpose of Processing The described processing activities are required for the legal division to administer the European Patent Register.

Data Retention For reasons of legal certainty, personal data is kept for an indefinite period.

Data subjects and categories of personal data

Externals

Ticketing	
Ticket related data	
Health Data	
Health Data	
Contact Information	
Contact Details	Phone Numbers
Working email address	
European Patent Register Data	
Address	Data provided by the data subjects
Correspondence	
Personal information provided voluntarily	
Patent Process Related Data	
Personal data potentially included within the content of a patent (claims, description, drawings, abstract)	
Financial	
Bank Account Information	Bank Account Number
Credit Card Number	Debit Card Number
Employment Information	
Business Unit Division	Company Entity
Department name and/or number	Job Title Role
Language preference (of communication)	Office Location
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name

Gender	Surname
Nationality	Picture
Signature	
Government Identifiers	
National Identity Card Details	Passport Number

Employees

Contact Information	
Contact Details	Phone Numbers
Employment Information	
Business Unit Division	Job Title Role
Office Location	Personnel Number
Personal Identification	
Full Name	Signature

Recipient of the personal data

Recipients of the data 1) EPO internal Madras users
2) The public
3) trustees outside Member States.

Purpose of sharing 1) EPO internal Madras users have access to all data filed thereof.

2) The public has access to the data that is visible in the European Patent Register.

3) In some Rule 142 EPC cases, trustees outside Member States are notified of the information published in the European Patent Register.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) Derogation in accordance with Art. 10 DPR

Country where data might be transferred - Processor (Vendors) ServiceNow - Netherlands, Microsoft - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, Informing Trustees is part of the European Patent Register tasks

Derogations Art. 10 DPR The transfer is made from a register which, according to the legal provisions of the European Patent Organisation, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down for such consultation are fulfilled in the particular case, The transfer is necessary for the performance of a task in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning, or to perform obligations arising from its duty of co-operation with the contracting states

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 76

Name SACEPO meetings

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 41 - Finance, DG4 - 46 - CIO / BIT

Entity Name - Controller (Entities) DG5 - 52 - Legal Affairs

External processors

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

SAP

External processors	
Name SAP	

OpenText

External processors	
Name OpenText	

Members of Sacepo

External processors

Name
Members of Sacepo

Microsoft

External processors
Name
Microsoft

Description of the processing

Description A dedicated advisory body, the Standing Advisory Committee before the European Patent Office (SACEPO), was created in 1978 at the same time as the Office opened its doors, in order to involve users in the development of the European patent system. SACEPO brings together a wide range of experienced patent attorneys and representatives of industry (including small and medium-sized enterprises) to conduct a general review of EPO activities of the past year and projects for the future. Regular meetings hosted by the EPO President are held once a year. In addition, meetings of five specialist SACEPO Working Parties (Quality, Rules, Guidelines, Patent Information and E-Patent Process), dedicated to more technical matters, take place on a regular basis during the year.

The relevant personal data of SACEPO members, already collected during the SACEPO membership selection process, are used by the delegated controller to organise the above mentioned meetings.

All email exchanges as from the preparatory phase of the meetings until the following up exchanges after those, including sharing of minutes, are conducted through the SACEPO mailbox (SACEPO@epo.org) of the delegated controller.

The meetings are chaired/run by the President of the EPO or another EPO representative. Corresponding preparatory and follow-up or reporting phase requires the sharing of information through the electronic means used by the Office, such as e-mail and OpenText. Further EPO staff or, exceptionally, external experts are present as and when needed. MS Teams collaborative platforms can be set up to facilitate engagement between the participants to those meetings (SACEPO members and experts, and EPO senior experts/team managers).

While meetings occur virtually since the covid pandemic, physical meetings remain possible. Should the travel and/or accommodation costs of SACEPO's members be borne by the EPO, corresponding form would have to be filled and accompanied by justification documents. Should the Office organise a lunch or dinner, the participants might be asked about dietary needs.

After the meetings, the anonymous minutes are distributed to attendees via email. Other additional information related to the content of the presentations/discussions is usually distributed also.

Purpose of Processing The processing is necessary to plan, organise and run the consultation of the users of the patent system by this dedicated advisory body, the Standing Advisory Committee before the European Patent Office (SACEPO), created in 1978 This encompasses: 1. Organisation and holding of the meetings 2. Distribution of documents, agendas and minutes related thereto 3. In case of physical meeting, data necessary for e.g. reimbursement of travel and accommodation, dietary requirements 4. In case of virtual meetings, technical support as might be necessary 5. Preparation of the meetings by the EPO's officials involved. 6. Keep track of the consultation process for future reference and archiving.

Data Retention Should dietary requirements have been collected, this data is deleted after the event and latest after 3 months

Should invoices be sent to the delegated controller, (the case be) Invoices are kept for three years.

Other personal data of members of SACEPO processed in relation to those users' consultations is kept for three years after the elapsing of their SACEPO membership.

The anonymous Minutes of SACEPO meetings are kept without limitation of time.

Data subjects and categories of personal data

Employees

Matter/Log file	
Attachments	Metadata
Health Data	
Dietary requirements	
Contact Information	
Contact Details	Working email address
Employment Information	
Business Unit Division	Job Title Role
Personal Identification	
First Name	Gender
Surname	

Externals

General	
User association	
Ticketing	
Ticket related data	
Health Data	
Dietary requirements	
Contact Information	
Contact Details	Home Address
Phone Numbers	Working email address

Professional Experience & Affiliations	
CV	Professional Memberships
Qualifications Certifications	
Correspondence	
Personal information provided voluntarily	
Financial	
Bank Account Information	
Employment Information	
Business Unit Division	Company Entity
Job Title Role	Office Location
Personal Identification	
First Name	Surname
Nationality	

Recipient of the personal data

Recipients of the data - Internal participants to the meetings
- External participants, business associations whose delegates are SACEPO members
- Presenters and EPO senior management
- Technical Services
- Financial services
- External providers

Purpose of sharing - Sharing with participants is necessary to achieve the main purpose of the meetings (e.g. list of participants, minutes, documents)
- Upon request of interested parties, such as business associations whose delegates are SACEPO members, the EPO might decide to share the SACEPO meetings' material (agenda, documents, minutes) with those.
- EPO Presenters and EPO senior management share a meeting file including background on participants
- Technical Services (if necessary; only relevant contact data is shared)
- Financial services (as necessary for reimbursements)
- External contractors for service providing.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards, Derogation in accordance with Art. 10 DPR

Country where data might be transferred - Processor (Vendors) Microsoft - United States, OpenText - United Kingdom, SAP - Germany, TRE Thomson Reuters - Luxembourg

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, International cooperation activities

Derogations Art. 10 DPR The transfer is necessary for the performance of a task in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning, or to perform obligations arising from its duty of co-operation with the contracting states

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 77

Name Disciplinary procedures against professional representatives before the EPO

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 44 - General Administration

Entity Name - Controller (Entities) DG5 - Chairman of the Disciplinary Board of the EPO

External processors

zoom

External processors	
Name zoom	

Zoom

External processors	
Name Zoom	

OpenText

External processors	
Name OpenText	

Microsoft

External processors

Name
Microsoft

External member of Disciplinary Board if outside the EEA

External processors
Name
External member of Disciplinary Board if outside the EEA

Data subject or his representative if located outside EEA

External processors
Name
Data subject or his representative if located outside EEA

Zoom

External processors
Name
Zoom

External members of the Disciplinary Board of the EPO

External processors
Name
External members of the Disciplinary Board of the EPO

Microsoft

External processors
Name
Microsoft

Zoom

External processors
Name
Zoom

zoom

External processors
Name
zoom

Description of the processing

Description Infringements of the Rules of Professional Conduct of Professional Representatives may be considered by the following bodies (See Article 5 Regulation on discipline for professional representatives; hereafter “RegDisc” as well as Additional Rules of Procedure of the Disciplinary Board of the European Patent Office hereafter “AddRules”):
(a) the Disciplinary Committee of the Institute of Professional Representatives before the European Patent Office (hereinafter “DC of the EPI”)
(b) the Disciplinary Board of the European Patent Office (hereinafter DB of the EPO)
(c) the Disciplinary Board of Appeal of the European Patent Office (hereinafter DBoA)

(a) Involvement in procedure with the Disciplinary Committee of the EPI
The Chair and the registrar of the DB of the EPO are involved incidentally during proceedings with the DC of the EPI (item (a) above). The processing operation is triggered by the receipt of the notification by the Disciplinary body of the EPI, to allow the application of Article 6 RegDisc, per email. These provisions require the close involvement of the chairman and of the registrar of the DB of the EPO, monitoring time lines and taking decisions of procedural nature. A corresponding file is created by them in a confidential shared-drive. This involvement leads either to the closure of the case or to a further processing, should the matter be brought before the Disciplinary Board of the EPO:Procedure with the Disciplinary board of the EPO.

(b) Procedure with the Disciplinary board of the EPO

This procedure is triggered either by a decision of the DC of the EPI or by the chairman of the DB of the EPO (Article 6 RegDisc). The transmission of the relevant file from the DC of the EPI to the DB of the EPO as well as the information of the professional representative are regulated by Article 6 AddRules. The professional representative concerned can also be requested to provide directly further information/documents. This collection of personal data takes place via email or registered post. The registrar stores those in the dedicated mailbox (disciplinaryboard@epo.org) and computer, and stores the file in a dedicated shared-drive.

The operations necessary for the procedure with the DB of the EPO encompasses:
- Launching the procedure, information of DB members, conduct of preparatory inquiries, designation of rapporteur, organising the exchange of written submissions by the parties,
- the holding of oral proceedings in person or in virtual environment (video conferences), which necessitate the drafting of minutes and might involve the audio recording of the meeting (See e.g. Art 7 AddRules),
- the participation of further data subjects such as witnesses, legal practitioner, interpreters, President of the EPI, President of the EPO,
- All activities of the DB of the EPO, including deliberations, voting, decision making, necessitating regular meetings in person or in virtual environment (video conferences).
The video conferences may take place via Zoom or Teams.

This procedure ends with the final decision of the DB of the EPO to dismiss the matter or to impose penalties. The decision might have to be notified to the Legal division of the EPO (Art 28(2) RegDisc), or be published under certain conditions and in an anonymised way as provided in the applicable rules (Art 16 AddRules). The final decision means the end of the active processing of the file by the DB of the EPO.

(c) Procedure with the DBoA
The DB is not involved in this procedure.

Purpose of Processing The personal data is processed to enable the Disciplinary Board of the EPO or, the case be, its chairperson or registrar, to perform the tasks with regard to the discipline against Professional Representatives (See Regulation on discipline for professional representatives (OJ EPO 1978, 91, OJ EPO 2008, 14); Additional Rules of Procedure of the Disciplinary Board of the European Patent Office OJ EPO 1980, 183 OJ EPO 2007, 552, 555) which encompass - Organising and monitoring administrative steps to allow o timely and informed Decisions, as foreseen in the applicable provisions o planning and organising the work of the DB of the EPO o report on these activities when required, including with the provision of anonymous statistics - keep track of past decisions in case the same individual is involved in or subject of further disciplinary procedures, or in case of related litigation. - Keep track of past procedures to allow an harmonised and consistent approach of the DB, also to ensure legal certainty.

The files of the DB of the EPO are kept until the end of the applicable retention period(s).

Data Retention In cases not leading to a disciplinary sanction, the retention time is 5 years from the date of the decision of the DB.

In case leading to a disciplinary sanction, the retention time is 10 years from the date of the decision of the DB.

However, should a related litigation have been launched and the above time line have elapsed, the file is kept for 5 years after the end of the litigation.

After the elapsing of the applicable retention time, only the complaint and the decision are kept.

The minutes are submitted to the parties prior to their adoption. Once the minutes adopted, the recording is deleted.

Data subjects and categories of personal data

Externals

Health Data	
Health Data	
Contact Information	
Contact Details	Home Address
Personal Email	Phone Numbers
Working email address	
Professional Experience & Affiliations	
CV	Political Affiliation and Activities
Professional Memberships	Qualifications Certifications
European Patent Register Data	
Address	Data provided by the data subjects
Correspondence	
Personal information provided voluntarily	
Patent Process Related Data	
Personal data potentially included within the content of a patent (claims, description, drawings, abstract)	
Employment Information	
Company Entity	Job Title Role
Language preference (of communication)	Office Location

Previous Work History	
Personal Identification	
Age	Date of Birth
Disability or Specific Condition	First Name
Full Name	Gender
Surname	Nationality
Picture	Signature

Employees

Contact Information	
Contact Details	Home Address
Phone Numbers	Working email address
Employment Information	
Room Number	
Personal Identification	
Digital signature	Full Name
Signature	

Recipient of the personal data

Recipients of the data Respondent(s) of the disciplinary case (professional representative against whom the breach of the Rules of professional Conduct is alleged), representative of respondent of the disciplinary case.
Chairman of the DC of the EPI (see e.g. Art 6 RegDisc), Presidents of the EPO and of the Council of the Institute of professional representatives (see e.g. Art 12, 14 and 21 RegDisc):
External disciplinary Board members (access to the whole file).

The president of EPI receives the decision according to Art 21 RegDisc) as well as communication giving him the opportunity to comment before final decision is taken Art 12 RegDisc
BoA receives the DB cases from DB of the EPO in case an appeal is filed to a DB decision
Complainant / or representative of complainant is informed of the result of the proceedings (Art21 RegDisc)
Respondent as well as their representatives receive the decision as well as communication giving him the opportunity to comment before final decision is taken Art 12 RegDisc
The case be, interpretors

Note: The internal disciplinary board members, the registrar of Disciplinary board and staff of D523 supporting the Chairperson in the exercise of this independent function are considered as belonging to the delegated controller's unit for the purpose of this record, and are thus neither considered as recipients or internal processors.

Purpose of sharing

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards, Derogation in accordance with Art. 10 DPR

Country where data might be transferred - Processor (Vendors) zoom - Unknown, Zoom - United States, Microsoft - United States, OpenText - United Kingdom

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, Communication with data subjects or their representatives, Performance of activities of the Disciplinary Board

Derogations Art. 10 DPR The transfer is necessary for the performance of a task in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning, or to perform obligations arising from its duty of co-operation with the contracting states

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data

protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 78

Name Selection of members of the Disciplinary board of the Office

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG5 - 53 - Patent Law and Procedures

External processors

OpenText

External processors	
Name OpenText	

OpenText

External processors	
Name OpenText	

Microsoft

External processors	
Name Microsoft	

Microsoft

External processors

Name
Microsoft

Description of the processing

Description According to Article 9(2) of the Regulation on discipline for professional representatives (the Regulation), the members of the Disciplinary Board of the EPO ("DB of the EPO") are appointed by the President of the Office for a period of three years. The board consists of legally qualified members of the EPO and of professional representatives (Article 9(1) of the Regulation).

The professional representatives are selected from a list proposed to the president by the Board of the Institute of professional representatives before the European Patent Office (epi). For this purpose, epi is reminded by Legal Affairs/D523 to propose a list of potential members.

The processing of personal data is triggered by the receipt, usually by post, of the list sent by the epi. Legal Affairs proceeds with the checking of the formal conditions required for the appointments and the setting up of the board(s). It prepares the file for the decision of the President, entailing the names proposed by the epi as well as proposing names of Office's legally qualified employees which could be (re-)appointed. The file is sent to the President of the Office for decision via CommonLog (CL).

Once the decision(s) taken be the President, usually with prior consultation of either Director 523, PD5.2, CILO and/or VP5, the newly appointed members of the disciplinary board are informed via an Appointment letter signed by the President sent by D523 via post. The epi is informed of the names of its proposed members having been appointed. The appointments are also published in the Official Journal. The business distribution scheme might also be published in the Official Journal.

The active processing of this data stops after the appointment.

The selection file is kept in the CL according to the retention times prevailing therein. A copy of the file is kept in Legal Affairs/D523 by the registrar of the Disciplinary board on a shared drive with restricted access. Only the registrar, the deputy registrar and the chairperson of the Disciplinary board have access to the shared drive.

Data Retention The retention period is 10 years, unless any of the cases handled by the members of the DB appointed via this procedure is subject to a litigation. In such event, should the 10 years retention period be over, the data might be kept for 5 years after the end of the litigation.

The retention period for the data of unsuccessful candidates is 3 years.

Purpose of Processing The processing is necessary to select and appoint the members of the disciplinary board of the EPO (Article 9(2) of the Regulation on discipline for professional representatives). This encompasses: - publication of the appointments - Use the contact data of appointed members for the organisation of the DB meetings - Ensuring legal certainty with regard to the lawfulness of the selection procedure of the DB of the EPO - providing the Office with a pool of potential internal and external candidates for next selections

Data subjects and categories of personal data

Externals

Contact Information	
Contact Details	Home Address
Personal Email	Phone Numbers

Working email address	
Professional Experience & Affiliations	
CV	Professional Memberships
Correspondence	
Personal information provided voluntarily	
Employment Information	
Company Entity	Office Location
Personal Identification	
Full Name	Nationality

Employees

Contact Information	
Contact Details	Working email address
Professional Experience & Affiliations	
CV	
Employment Information	
Job Title Role	Room Number
Personal Identification	
Full Name	Nationality

Recipient of the personal data

Recipients of the data
Office's employees involved in the selection and decision-making process, on a strict need-to-know basis (usually Director 523, PD5.2, CILO and/or VP5, President of the Office, registrar of the disciplinary board).

The public (names only) via DG5 Editorial Office which publishes the names of the newly appointed members in the EPO Official Journal; the epi is informed separately of the appointment of the Professional Representatives.

Purpose of sharing strict need-to-know basis

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors)
Microsoft - United States, OpenText - United Kingdom

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 79

Name Organisation of meetings with the US Bar-EPO liaison Committee

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG5 - 52 - Legal Affairs

External processors

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

OpenText

External processors	
Name OpenText	

US Bar Liaison Office

External processors	
Name US Bar Liaison Office	

Microsoft

External processors

Name	
Microsoft	

Description of the processing

Description The US Bar-EPO Liaison Council was created as a forum to facilitate exchange between the EPO and US applicants. It serves to increase mutual understanding of European and US patent practice, and update members on recent developments on both sides of the Atlantic.
The US Bar-EPO Liaison Council is an US Organisation with its own statutes, created by US Stakeholders in 1984. The annual meetings usually take place alternately at the EPO and in the US.

When the meeting takes place at the EPO, the personal data necessary to the organisation of the meetings, including professional background of participants, is requested by D522 from the US Bar-EPO Liaison Council Chair. Other participants are usually Office employees. The requested information is usually received via email.

The data, received by email and manually stored on the w: drive, is used by the EPO (Dir 522) to organise the meeting and communicate all related information. Standard EPO tools are used: Microsoft Office 365, CMS (Case Management System) of legal affairs (see dedicated record), OpenText.
This includes sharing information with relevant stakeholders:
- Technical aspects to be dealt with for the meeting itself (e.g. digital platform)
- Exchanges prior to the meeting, e.g. for the preparation of the agenda, presentations, and president meeting file. D.522 liaises with the President's Office for the date and the file and the Protocol unit, should there be meals organised at an in-person meeting.
- Exchanges after the meeting, including sharing presentation materials, and other EPO documents, possible follow-up actions etc
- In case of physical meeting with organisation of a dinner, additional personal data might be processed related to dietary requirements provided on a voluntary basis by the participants.
- The list of US delegates is sometimes used to identify US candidates for SACEPO.

Data Retention - Meeting files and emails are stored for 20 years. Particularly important files might be archived beyond this time period.

- The Excel tables containing contact data are destroyed after 10 years.

- Should dietary requirements have been collected, this data is deleted after the event and latest after 3 months

Purpose of Processing Allow informal exchanges between the EPO and US applicants with a view to increase mutual understanding of European and US patent practice and to update members on developments on both sides of the Atlantic. This encompasses: - Setting up of physical or virtual meetings - Keeping track of previous exchanges and of related context - Plan future events - Maintain a database of experts in US patent law for future consultation, including in order to select potential US participants in SACEPO.

Data subjects and categories of personal data

Employees

Matter/Log file	
Attachments	Metadata
Health Data	
Dietary requirements	
Contact Information	

Contact Details	Working email address
Correspondence	
Additional Information which might be provided in the course of exchanges	
Employment Information	
Business Unit Division	Job Title Role
Personal Identification	
First Name	Surname

Externals

Matter/Log file	
Attachments	Metadata
General	
Any other information	User association
Health Data	
Dietary requirements	
Contact Information	
Contact Details	
Professional Experience & Affiliations	
CV	Professional Memberships
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Employment Information	
Company Entity	Job Title Role
Personal Identification	
First Name	Surname

Recipient of the personal data

Recipients of the data - Chair of the US Bar-EPO Liaison Council, internal (EPO) participants (usually from DG1 and DG5) and external participants of the US Bar Liaison Office.

- Senior managers of the Office, usually President of EPO, Vice-Presidents DG1 and DG5, Chief International and Legal Officer.

- Presenters (internal EPO employees, usually from DG1 and/or DG 5), selected for their expertise in the field(s) to be discussed at a meeting.

Purpose of sharing - Chair of the US Bar-EPO Liaison Council, internal (EPO) and external participants of the US Bar Liaison Office: list of participants and documents shared as a preparation or follow up of a meeting.

- Senior managers and EPO presenters have access to the meeting file (Common Log) drafted within the delegated controller's principal directorate and submitted to the President of the Office for the sake of the organisation and preparation of the meeting. This entails information on participants and their professional background.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards, Derogation in accordance with Art. 10 DPR

Country where data might be transferred - Processor (Vendors) TRE Thomson Reuters - Luxembourg, Microsoft - United States, OpenText - United Kingdom

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, International cooperation activities

Derogations Art. 10 DPR The transfer is necessary for the performance of a task in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning, or to perform obligations arising from its duty of co-operation with the contracting states

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 81

Name Legal advice on contractual, (pre-)litigation and other general matters by Directorate 5.2.4 – Contract law and litigation

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG5 - 52 - Legal Affairs

External processors

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

Microsoft

External processors	
Name Microsoft	

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

External Law Firms

External processors

Name
External Law Firms

Microsoft

External processors
Name
Microsoft

Description of the processing

Description D524 receives requests from other EPO units requesting for legal advice in contractual, litigation and general matters. Such requests are received by D524 via e-mail (e. g. Outlook), orally or in writing. All requests are registered in the Case management System (CMs) of the Directorate under a specific Log number together with the requester's and responsible officer's names and assigned to a responsible lawyer within the Directorate.

Once the request has been assigned to the responsible lawyer the legal question is identified, assessed, and answered to the requester via e-mail, orally or in writing.

The CSM is subject of a separate record.

Purpose of Processing Personal data is processed for the purpose of the EPO's administrative functioning, here in particular providing legal advice on matters within the responsibility of D 5.2.4: • giving Legal advice on matters of contractual and general legal nature, such as private and public building / construction law and all aspects of IT law, as well as memoranda of understanding and service level agreements; • identify and manage the legal risks which the Office faces in its activities; • support colleagues in the operational units and in Central Procurement in procurement matters, in particular in the preparation, drafting, negotiation and implementation of contracts; • vetting of contracts and CA documents according to Art. 1 ff of the Directive on contracts • assisting the operational units with the appropriate management of contracts, helping monitor the legal aspects to prevent issues before they arise; • maintaining an up-to-date, fit-for-purpose database of model contracts in different areas; • providing training and information on legal matters to stakeholders across the Office; • providing legal advice and support relating to litigation issues (with the exception of employment disputes), including on the avoidance of litigation (mediation, settlement), and oversee and coordinate any litigation efforts; • legal administration and management of the portfolio of intangible assets of the Office, such as trademarks and copyrights. • supporting the realisation of the Strategic Plan 2023, and assisting in the associated programmes and projects. • assisting in the managing and distribution of files and coordinating follow-up activities, as well as for accountability purposes. This is necessary for giving legal advice. Relevant provisions are: Rule 3.2 Tender Guidelines, point 6.5.2 of the Directive supplementing certain provisions of the Tender Guidelines, Directive on contracts.

Data Retention Personal data processed are stored for the period of time necessary to achieve the purpose for which they have been processed.

contract related files:

D 5.2.4 is asked to advise on drafting of a contract (see “Definitions” section in the Directive on contracts) and issues a legal approval for a given contract, and this contract is also concluded between the EPO and the contractor. D 5.2.4 physically destroys the corresponding file 12 years after termination of this contract (e. g. contract concluded on day 0 for delivery of items six weeks later, items are delivered 8 weeks later, file is destroyed 12 years after performance; framework contract concluded on day 0 for duration of five years, terminated already after 3 years, file is destroyed 12 years after termination)

all other cases:

D 5.2.4 gives a general legal advice that is not covered by the description above. File is physically destroyed 30 years after completion of this file.

Data subjects and categories of personal data

Employees

General	
Any other information	Assessment and legal opinions
Contact Information	
Personal Email	Phone Numbers
Working email address	
Correspondence	
Any other information	Personal information provided voluntarily
Employment Information	
Assessment and legal opinions	Business Unit Division
Personal Identification	
First Name	Surname

Externals

General	
Any other information	Legal opinions and assessments

Contact Information	
Home Address	Personal Email
Phone Numbers	
Correspondence	
Any other information	Personal information provided voluntarily
Personal Identification	
First Name	Surname

Recipient of the personal data

Recipients of the data Personal data will only be shared on a strictly need to know basis.

In general, personal data may be included in various communications or legal documents sent within the EPO for information and consultation of operational units or involved employees for the purpose described above.

In case of consultation of a law firm, D524 might have to share personal data with them.

Purpose of sharing In general, personal data may be included in various communications or legal documents sent within the EPO for information and consultation of operational units or involved employees for the purpose described above.

In case of consultation of a law firm, D524 might have to share personal data with them.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards, Derogation in accordance with Art. 10 DPR

Country where data might be transferred - Processor (Vendors) Microsoft - United States, TRE Thomson Reuters - Luxembourg

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, External law firms providing legal consultancy services

Derogations Art. 10 DPR The transfer is necessary for the performance of a task in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning, or to perform obligations arising from its duty of co-operation with the contracting states

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 82

Name Maintenance of List of professional representatives

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG5 - 53 - Patent Law and Procedures

External processors

ServiceNow

External processors	
Name ServiceNow	

Microsoft

External processors	
Name Microsoft	

Uniwise APS

External processors	
Name Uniwise APS	

Microsoft

External processors

Name
Microsoft

ServiceNow

External processors
Name
ServiceNow

Description of the processing

Description A natural person (external) must be registered on the list of professional representatives to be entitled to act as a professional representative before the EPO.

The Legal Division is responsible for:
- decisions on registration on and deletion from the list of professional representatives in accordance with Articles 20 EPC, 134 EPC, Rule 154 EPC, the notice from the EPO of 12.05.2015 concerning representation before the EPO (OJ EPO 2015, A55) and the decision of the President of the European Patent Office dated 21 November 2013 concerning the responsibilities of the Legal Division, OJ EPO 2013,600,
- entry in the European Patent Register, Rule 143(1)h EPC,
- entry in the EPO searchable database.

The request for entry on the list of professional representatives is related to the passing of the EQE exams, apart from special circumstances such as accession of a State to the EPC. Relevant personal data is collected from the data subjects via specific forms (EPO Form 52300 or 53203), to be sent to the legal division in paper form together with supporting documents. Alternatively, the request can be done online using an electronic platform.

The deletion from the list of professional representatives is either triggered by a request (preferably using EPO form 52306) or information from the Institute of Professional Representatives before the EPO (epi) (deletion ex officio), the disciplinary board, or others (e.g. dependants, employer). For the processing of deletion from the list of professional representatives, special documents (including personal data and, possible special categories of personal data) are required depending on the grounds of the deletion.

The maintenance and publication of an up-to-date information status is one of the main activities performed. Any change of name/address or other details in the list of professional representatives before the EPO must be sent to the EPO Legal Division, preferably using EPO Form 52301 and 53201a.

The legal division provides other Office's units or external stakeholder (epi) with relevant information necessary to perform tasks associated with being a professional representatives, e.g. to ensure the publication, preparation of EPO badges for professional representatives, to allow invitation to specific events, seminars, surveys etc. Other contact detail exports or statistics can be provided internally, on request.

Most personal data are provided by the professional representatives themselves. Other sources apply sometimes, such as lists of successful candidates by EQE or information provided by epi.

System description:
Documents are usually received by post or email. All paper documents are scanned, sent in pdf format via Outlook (generic email address of

Purpose of Processing The processing of personal data is necessary for the setting up, maintenance and publication of the list of professional representatives by the Office and providing up-to-date information to stakeholders as well as all associated actions to e.g. ensure a proper and efficient information flow and management of associated activities. This encompasses: – Entry on, and deletion from, the list of professional representatives and in the European Patent Register – publication in the EPO Official Journal, Announcement of the list of professional representatives before the EPO, publication on the searchable database – ensuring that the Institute of Professional Representatives before the EPO is provided with the personal data necessary to administer the data subjects' Institute membership, intrinsically related to being entered on the list of professional representatives – provide Office's units with information necessary to perform tasks associated with being listed as professional representatives - Preparation of statistics

the legal division) and stored in folders by date. These PDF-documents are stored in the D523 Tele-Archive folders sorted by date, name, CDS ID number, filing number and country on the EPO Shared-Drive (w: drive). Entry requests and the deletion procedure ex officio are monitored via Excel files on the EPO Shared-Drive (w: drive). Those files are only accessible by the legal division.
The legal division enters the relevant data in the database CDS (Client Data System, part of Madras, owned by Directorate-General 1), used mostly by formality officers.
CDS generates an ID-Code for each new entry of a professional representative. Furthermore, CDS records history data of actions and links the professional representative role to relationships like membership of a registered association or appointment as an authorisee in a general authorisation. CDS is used by DG1 to combine several types of information about different roles, acting addresses, including the link to dedicated filings. The Legal Division is the sole data owner of the role of professional representative and the main address in CDS. Any change of data or status could have direct impact on the representation in patent procedures (DG1). A daily export of the data of professional representatives is retrieved from CDS to DG5Admin, which is an application built on the Microsoft stack, using .NET, IIS, SharePoint, and Excel with VBA, hosted by the EPO Data Centre in Luxembourg. The export includes the number of applications linked to the professional representative, which is used for analytical statistics, like the number of most active representatives. DG5Admin processes data, statistics, exports, data consent registration and is generating Share point templates and Word documents. In addition, an Excel statistic template is used to generate anonymous figures about the actions performed in CDS, trigged by action date and type of change.

Data Retention For reasons of legal certainty, personal data is kept up to 99 years, starting from the first entry date on the list of professional representatives.

Data subjects and categories of personal data

Externals

Ticketing	
Ticket related data	
Health Data	
Health Data	
Contact Information	
Contact Details	Phone Numbers
Working email address	
Professional Experience & Affiliations	
Professional Memberships	Qualifications Certifications
European Patent Register Data	
Address	Data provided by the data subjects
Correspondence	

Personal information provided voluntarily	
Representation in EPO's Patent Granting Process	
Affiliation to Association of professional representatives	All data provided upon request for entry or change
Authorisee function	Authorisor function
EPO CDS (Client Data System) categories related to the Representation role	Role in the Patent Grant Procedure
Supporting documentation	
Browsing Information	
IP Address	
Employment Information	
Business Unit Division	Company Entity
Job Title Role	Office Location
Previous Work History	
Personal Identification	
Age	Date of Birth
First Name	Full Name
Gender	Surname
Nationality	Signature
Government Identifiers	
National Identity Card Details	Passport Number

Employees

Ticketing	
Ticket related data	
Contact Information	
Phone Numbers	Working email address
Employment Information	
Business Unit Division	Job Title Role
Office Location	Personnel Number

Personal Identification	
Full Name	Gender

Recipient of the personal data

Recipients of the data Apart from the publicly available data published in the OJ and/or in the searchable database of the EPO:

Different business units at the EPO will have access to the information stored on the list of professional representatives on a need to know basis:

• DG5 Editorial Office: EPO Official Journal (name, former name if applicable, nationality, address, deletion reason indication like death)
• DG5 Publication European Patent Bulletin (EPB): Public notification of decision if its delivery has proven to be impossible
• DG4 Online Solutions Team: Online database of professional representatives (according to consent form public data)
• DG4 Access card management system: Nexus Prime application for issuing the EPO badges (following data is export from DG5 to DG4: name, surname, email address, CDS ID code, entry and deletion date from the list of professional representatives)
• DG1 Central Enquiries Unit (Support): CSM-Ticket database (CSM: Customer Services Management system)
• DG1 has access to CDS and CDR (PA DG1) receives copy of change requests (PDF-Files) in Shared drive folder
• Other internal contact detail exports or statistics on request for DG0, DG1, DG5
• Other involvements: Board of Appeals in case of an appeal (paper copy)

Institute of professional representatives, regular data transmission regarding the status of the professional representative and the membership payment of epi subscriptions.

Purpose of sharing Fulfil the purpose of the existence of the list of professional representatives.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards, Data Protection EU Comm Standard Contractual Clauses

Country where data might be transferred - Processor (Vendors) ServiceNow - Netherlands, Microsoft - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 83

Name Activities related to pre-litigation and litigation on civil service matters where the Administrative Council is competent appointing authority

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 44 - General Administration

Entity Name - Controller (Entities) DG5 - 52 - Legal Affairs

External processors

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

OpenText

External processors	
Name OpenText	

External Law Firms

External processors	
Name External Law Firms	

OpenText

External processors

Name
OpenText

Microsoft

External processors
Name
Microsoft

Microsoft

External processors
Name
Microsoft

External Law Firms

External processors
Name
External Law Firms

Description of the processing

Description Administrative and judicial means of redress are available to EPO staff.

Where a dispute involves the Administrative Council as appointing authority, Legal Affairs assists by providing case management and legal services at pre-litigation (management review and appeal) level. This includes :
- collecting relevant facts and evidence, analysing and advising on the case
- preparing documents to be submitted to the Council
- preparing submissions to be submitted on its behalf by PD 52 acting as representative in internal appeal proceedings
- assisting in alternative dispute resolution attempts.

if a case reaches litigation level, the Organisation is represented by another unit in the judicial proceedings before the ILOAT. Legal Affairs will at this stage provide assistance to the representative and prepare any documents to be submitted to the Council in relation to the case.

For this activity, personal data of the persons directly or indirectly involved in a dispute (mostly staff members, former staff members or their dependents as claimants but also legal representatives, witnesses, case handler etc.) are processed.

Information related to a case, including personal data, are collected via pleadings and evidence submitted from the parties to proceedings, third parties (e.g. witnesses), publicly available sources (e.g. internet searches), or gathered from other Office's units in the course of fact-finding activities when preparing a case (e.g. HR, manager). The personal data collected from the parties' submissions can be about them or others. The personal data so collected may occasionally include special categories of data. The categories of personal data processed depends on the subject matter of a case.

Information related to a case is stored electronically in a document management system and in the files kept by Legal Affairs. In some cases, a paper file is created.

Information related to a case are used in documents produced along the proceedings and exchanged between the parties or submitted to consultative (Appeals Committee) and decision-making (Administrative Council) bodies.

Information related to a case is shared within the Office as necessary for example to allow verification of factual elements, to inform or consult other services, to request translation, or in the course of approval process.

Information related to a case is transmitted outside the Office as necessary, for example when an external attorney is involved or other experts are consulted (e.g. tax expert).

References to cases are included in lists kept for monitoring pending litigation, for reporting and for statistical purposes.

Purpose of Processing Personal data is processed for the purpose of the EPO's administrative functioning, here in particular: 1- for assisting and/or representing the Administrative Council throughout administrative or judicial proceedings initiated against its decisions. 2- enabling the availability of dispute files for later reference in the event of subsequent litigation 3 – for archiving and statistical purposes.

Data Retention Personal data processed are stored for the period of time necessary to achieve the purpose for which they have been processed.
In the absence of a specific reason to retain a file:
Litigation that led to a judgment from the ILOAT:
* 10 years after the judgment was pronounced the parts of the file relating to the precedent stages of litigation, are destroyed.

* 15 years after the pronouncement of the judgment, all parts are destroyed.

Litigation that did not lead to a judgment from the ILOAT:
* 10 years after the closing of the last internal stage of proceedings, all parts of the file other than the advisory opinion and the decision closing the stage of proceedings are destroyed.

* 15 years after the closing of the last internal stage of proceedings, all parts are destroyed.

This applies to both electronic and paper files.

An index of cases with limited personal data categories (reference, name, status) is kept indefinitely.

Data subjects and categories of personal data

Employees

General	
Assessment and legal opinions	
Health Data	
Health Data	
Contact Information	
Contact Details	
Professional Experience & Affiliations	
Trade Union Membership	
Correspondence	
Personal information provided voluntarily	
Family Information	
Children's Names	Parents' Names
Spouse's information	Spouse's name
Employment Information	
Appeals Records Information	Assessment and legal opinions

Benefits and Entitlements Data	Business Unit Division
Company Entity	Contract Type
Corporate Credit or Debit Card Numbers	Disciplinary Action
End Date and Reason for Termination	Exit Interview and Comments
Grade	Grievances and Complaints
Hours of Work	Job Application Details
Job Title Role	Line Reporting Manager
Military Status	Office Location
Performance Rating	Personnel Number
Previous Work History	Record of Absence/Time Tracking/Annual Leave
Salary	Start Date
Weight	
Personal Identification	
Age	Date of Birth
Disability or Specific Condition	First Name
Full Name	Gender
Height	Surname
Marital Status	Nationality
Racial or Ethnic Origin	Religion/Religious Beliefs
Sexual Orientation	Signature

Former Employees

Health Data	
Health Data	
Contact Information	
Contact Details	
Professional Experience & Affiliations	

Trade Union Membership	
Correspondence	
Personal information provided voluntarily	
Family Information	
Children's Names	Parents' Names
Spouse's information	Spouse's name
Employment Information	
Appeals Records Information	Benefits and Entitlements Data
Business Unit Division	Company Entity
Contract Type	Corporate Credit or Debit Card Numbers
Disciplinary Action	End Date
End Date and Reason for Termination	Exit Interview and Comments
Grade	Grievances and Complaints
Hours of Work	Job Application Details
Job Title Role	Line Reporting Manager
Military Status	Office Location
Performance Rating	Personnel Number
Previous Work History	Record of Absence/Time Tracking/Annual Leave
Salary	Start Date
Weight	
Personal Identification	
Age	Date of Birth
Disability or Specific Condition	First Name
Full Name	Gender
Height	Surname
Marital Status	Nationality
Racial or Ethnic Origin	Religion/Religious Beliefs

Sexual Orientation	Signature

Externals

Contact Information	
Contact Details	
Personal Identification	
First Name	Surname

Recipient of the personal data

Recipients of the data At all stages of pre-litigation and litigation, personal data can be included in diverse communications or legal documents sent:

- within the EPO:
- for information and consultation of operational units or staff members involved in the conduct of litigation, on a strict need-to-know basis (Administrative Council Chairman and Secretariat, Office's hierarchy, HR, Employment Law, Boards of Appeal Unit, Conflict Resolution Unit, Ethics and Compliance Unit)
- In case a translation is needed, to Language Services
- In the course of proceedings to decision-making (Administrative Council) and consultative bodies (Appeals Committee)

- possibly outside the EPO:
to external attorneys.

Purpose of sharing Operational units or staff members involved in the conduct of litigation (Administrative Council Chairman and Secretariat, Office's hierarchy, HR, Employment Law, Boards of Appeal Unit, Conflict Resolution Unit, Ethics and Compliance Unit): for fact-finding purposes, information and/or consultation

Language Services: for obtaining a translation.

Administrative Council and Appeals Committee: for the purpose of carrying out certain procedural actions.

Possibly: external attorneys for the purpose of seeking representation or assistance.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards, EC Adequacy Decision

Country where data might be transferred - Processor (Vendors) OpenText - United Kingdom, TRE Thomson Reuters - Luxembourg, External Law Firms - Switzerland, Microsoft - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 86

Name Microsoft Office365 applications

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG4 - 46 - CIO / BIT

External processors

Microsoft

External processors	
Name Microsoft	

Indra

External processors	
Name Indra	

Microsoft

External processors	
Name Microsoft	

Description of the processing

Description Office 365 is a cloud-based package of applications (Word, Excel, PowerPoint, Outlook, SharePoint Online, OneDrive, MS Teams, MS Forms and others also listed in the Product Terms, December 01, 2021) provided to users with the aim to offer more flexibility and improve communication, collaboration, as well as the availability of resources.

As mentioned above, the Office 365 package also includes MS Teams, its core features include business messaging, calling, audio and video meetings and file sharing. MS Teams is a cloud-based application to organise virtual meetings and teleconferences both within the EPO and between the EPO and EPO's stakeholders. The core capabilities in Teams include business messaging, calling, video meetings, and file sharing.

In addition to these core capabilities, MS Teams also allows the recording of virtual meetings and the use of live captions. The use of such features is granted to specific stakeholders in accordance with internal policies on the use of MS Teams. For instance, the possibility of recording a virtual meeting depends on the nature of the meeting and must be authorised by the Data Protection Liaisons (DPLs). Participants will be notified both in the invitation and before the recording is activated that the meeting will be recorded and will be informed about the possibility to object to the recording.

In addition, Office 365 also includes non-optional Connected Experiences which are designed to enable more effective creation, communication, and collaboration.

Personal data is processed, i.e. collected and stored in Microsoft's cloud servers, for the purpose of providing the above-mentioned services.

Purpose of Processing Microsoft Office 365 applications are used by EPO employees and contractors to fulfil their daily tasks. Within the scope of the present processing operation, PD4.6 Delegated Controller processes personal data for the following purposes: • Delivering MS Office 365 applications and services to the EPO's staff and contractors • Providing end-user support and troubleshooting for Microsoft 365 Office applications and features • Managing content uploaded to Microsoft Office 365 • Managing Microsoft Office 365 settings • Supporting, operating and maintaining the Microsoft Office 365 applications. Microsoft Office 365 apps may be used for a number of different, specific purposes and scenarios, which the present record does not take into account. Delegated Controller BIT PD4.6 is accountable only for the purposes of processing that are stated in the present record. Any EPO Delegated Controller may decide if/when/which Microsoft Office 365 app to use, in order to fulfill own business purposes, tasks and activities. The specific scenarios and purposes - established by a given EPO delegated controller other than BIT PD4.6 - fall into said delegated controller's accountability remit and are described in its related records.

Data Retention At all times during the term of EPO's contract with Microsoft, EPO has the ability to access, extract and delete the data stored in the applications. Microsoft will retain EPO data that remains stored in the applications in a limited function account for 90 days after expiration or termination of EPO's subscription so that EPO may extract the data.

After the 90-day retention period ends, Microsoft will disable EPO's account and delete the EPO Data and Personal Data within an additional 90 days, unless Microsoft is authorized under the contract with EPO to retain such data.

For Personal Data in connection with the applications, Microsoft will delete all copies after the business purposes for which the data was collected or transferred have been fulfilled or earlier upon EPO's request, unless authorized under the agreement with EPO to retain such data.

EPO specific retention policies:

OneDrive: personal data is automatically deleted from OneDrive one year after the user account has been deleted.

Teams Chats, Teams Channel Messages, One Drive and Sharepoint content are stored until EPO's termination of the contract with Microsoft as explained above. If a Chat or Message in Teams is deleted by a user (or if any content in OneDrive and Sharepoint is deleted by user), then it is retained for one year after the last modification date in an area only accessible by an administrator before a final deletion.

For Teams, the history of phone calls is kept for 90 days and can be seen by administrators; an end-user can only see a 30-day-long own list of own phone calls.

Recordings of Teams meetings made using the Recording feature are retained for a period of three months before deletion unless otherwise defined by the recorder. Recording of Live Teams events are kept for 180 days. Such recordings may be kept for longer than one year depending on the nature of the meeting, whereby the period of retention is defined in accordance with the purpose of the recording. If a recording becomes outdated or obsolete before the end of the retention period it will be deleted. The specific retention period is provided in a dedicated data protection statement and/or disclaimer which is sent with the invitation to the meeting.

For surveys done via Forms: the survey owner is responsible for defining, communicating and manually enforcing the retention he/she has decided.

Data subjects and categories of personal data

Contractors

Phone Call Information	
Called Phone Number	Caller's Phone Number
Phone Call Date and/or Time	Phone Call Duration
Phone Call Interaction History	Phone Calling History
Physical and/or Digital Identifiable Assets	

Mobile Device Name	Operating System Version
Workstation's Hostname (Physical or Virtual)	
Sensory and Electronic Information	
Audio Information	Presence Status
Visual Information	
Telephony Interaction Data	
Telephony Session Content	Telephony Session Details
Telephony Session Metadata	
Employment Information	
Company Entity	Department name and/or number
Job Title Role	Language preference (of communication)
Office Location	Room Number
Personal Identification	
Digital signature	First Name
Surname	Picture
Geolocation	
Geolocation Information	
Network/application Interaction Data	
Session content	Session details
Session metadata	
Contact Information	
Phone Numbers	Working email address
Device Management Data	
Account ID	Last Logon Time
Correspondence	
Additional Information which might be provided in the course of exchanges	Personal information provided voluntarily
Browsing Information	
Browser type	Browser User Agent

Browsing Date and Time	Browsing Time
Cookie Information	IP Address
Network Interaction History	URL
Website History	
User Account Information	
Account Age	Account Number
Membership Permissions	Ownership Permissions
User ID	
System Logs	
Audit Logs (a.k.a. Audit Trail)	File data (name, size and/or hash)
Ports	Registry data
Running Processes	System-, Application-, Security-related Server Logs
Transaction-related Details	Web Servers Logs

Employees

Phone Call Information	
Called Phone Number	Caller's Phone Number
Phone Call Date and/or Time	Phone Call Duration
Phone Call Interaction History	Phone Calling History
Physical and/or Digital Identifiable Assets	
Mobile Device Name	Operating System Version
Workstation's Hostname (Physical or Virtual)	
Sensory and Electronic Information	
Audio Information	Presence Status
Visual Information	
Telephony Interaction Data	
Telephony Session Content	Telephony Session Details
Telephony Session Metadata	

Employment Information	
Business Unit Division	Department name and/or number
Job Title Role	Language preference (of communication)
Line Reporting Manager	Office Location
Personnel Number	Room Number
Personal Identification	
Digital signature	First Name
Surname	Picture
Geolocation	
Geolocation Information	
Network/application Interaction Data	
Session content	Session details
Session metadata	
Contact Information	
Phone Numbers	Working email address
Device Management Data	
Account ID	Last Logon Time
Correspondence	
Additional Information which might be provided in the course of exchanges	Personal information provided voluntarily
Browsing Information	
Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
Cookie Information	IP Address
Network Interaction History	URL
Website History	
User Account Information	
Account Age	Account Number

Membership Permissions	Ownership Permissions
User ID	
System Logs	
Audit Logs (a.k.a. Audit Trail)	File data (name, size and/or hash)
Ports	Registry data
Running Processes	System-, Application-, Security-related Server Logs
Transaction-related Details	Web Servers Logs

Externals

Phone Call Information	
Called Phone Number	Caller's Phone Number
Phone Call Date and/or Time	Phone Call Duration
Phone Call Interaction History	Phone Calling History
Network/application Interaction Data	
Session content	Session details
Session metadata	
Sensory and Electronic Information	
Audio Information	Presence Status
Visual Information	
Contact Information	
Personal Email	Working email address
Correspondence	
Additional Information which might be provided in the course of exchanges	Personal information provided voluntarily
Telephony Interaction Data	
Telephony Session Content	Telephony Session Details
Telephony Session Metadata	
Browsing Information	
Browser type	Browser User Agent

Browsing Date and Time	Browsing Time
Cookie Information	IP Address
Network Interaction History	URL
Website History	
System Logs	
System-, Application-, Security-related Server Logs	Web Servers Logs

Recipient of the personal data

Recipients of the data Personal data is disclosed on a need-to-know basis to the following recipients:
• EPO staff and external users included in Office 365 applications used for the exchange of information (for instance, the participants to an MS Teams meeting or the sender and recipient(s) of an email exchanged in Outlook).
• EPO PD4.6 , Indra and Microsoft staff involved in the data processing necessary to provide the service.

For Office 365, in principle the majority of the service operations are automated in order to reduce the need for human access.

Microsoft staff does not have standing access to EPO data and any required access is for a limited time. Moreover, Microsoft employs least privilege access mechanisms to control access to EPO data.

Where a virtual meeting is recorded in Ms Teams, the recording may potentially be disclosed to the EPO as a whole, or outside the EPO, depending on the meeting. In either circumstance, the data subject will be duly informed by the meeting organiser of the details of the processing operation.

For surveys/forms/questionnaires organised by an Owner via MS Forms: questions and answers are stored in Microsoft cloud; access to a survey's submitted responses is available to the survey's owners only. In case of anonymous survey, no contact information about the respondent is included in the response. In case of confidential surveys (= non anonymous), the owner has access to the respondent's name, email address, date and time when the respondent opened the survey, and data and time when the respondent submitted the response.

Purpose of sharing In the present processing operation, personal data is shared with EPO staff, contractors and external users in order to enable them to perform EPO tasks and activities.

Personal data is shared with the external processors (Microsoft and Indra) and EPO PD4.6 for the following purposes:
· Delivering MS Office 365 applications and services to the EPO
· Support, operation and maintenance of MS Office 365 applications
· End-user support and troubleshooting for Microsoft Office 365 applications and features “

In addition Indra and EPO PD46 may process personal data for the following purposes:
· Managing MS Office 365 settings
· Security purposes

Microsoft also processes the data for business operations purposes for which Microsoft is a Data Controller: (1) billing and account management; (2) compensation (e.g., calculating employee commissions and partner incentives); (3) internal reporting and business modeling (e.g., forecasting, revenue, capacity planning, product strategy); (4) combatting fraud, cybercrime, or cyber-attacks that may affect Microsoft or Microsoft Products; (5) improving the core functionality of accessibility, privacy or energy-efficiency; and (6) financial reporting and compliance with legal obligations. More information on this processing can be obtained in Microsoft’s public documentation

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors)
Microsoft - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, Protection against malware, login to Azure Active Directory, error analysis, load balancing, diagnostics data, connected experiences, and processing for Microsoft’s business operations

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures For personal data processed on systems not hosted on EPO premises, the providers processing the personal data have committed in a binding agreement to comply

with their data protection obligations under the applicable data protection legal frameworks. The EPO has also carried out a privacy and security risk assessment. Any personal data in transit over public networks between the EPO and Microsoft, or between Microsoft data centres is encrypted by default. Personal data as part of any data that are provided to Microsoft by, or on behalf of, EPO through use of the Microsoft 365 services is encrypted at rest. Regarding the implementation of the encryption, Microsoft uses state of the art encryption technologies. Furthermore, Microsoft employs least privilege access mechanisms to control access to personal data which are part of data that are provided to Microsoft by EPO and role-based access controls are employed to ensure that access to such personal data required for service operations is for an appropriate purpose and approved with management oversight. For Microsoft 365 Applications any required access by Microsoft is for a limited time. Microsoft 365 applications implement and maintain multiple security measures for the protection of personal data as part of any data that are provided to Microsoft by EPO through use of the Microsoft 365 services, which encompass the following: organisation of information security (e.g., security ownership, security roles and responsibilities, risk management program), asset management (e.g. asset inventory and asset handling), human resources security (e.g. security training), physical and environmental security (e.g. physical access to facilities, physical access to components, protection from disruptions, component disposal), communications and operations management controls (e.g. operational policy, data recovery procedures, anti-malware controls, event logging), access control measures (e.g. access policy, access authorisation, least privilege, integrity and confidentiality, authentication, network design), information security incident management (e.g. incident response process, service monitoring) and business continuity management. Microsoft also implements and maintain appropriate technical and organisational measures for protection of any other personal data distinct from the one described above, which are described in Microsoft Security Policy. Microsoft 365 applications have been configured to preserve the confidentiality of the information by employing the measures listed above. In addition, anonymous access is not authorised. Any information you add to Microsoft 365, be it via chat, videoconference, or file sharing, will be available only to the specific users and groups indicated in section 4 above. Microsoft 365 applications are certified in several security standards, including ISO27001, SOC1 Type II, SOC2 Type II and ISO27018 Code of Practice for Protecting Personal Data in the Cloud and complies with the requirements set forth in ISO 27002. Microsoft conducts annual audits of the security of the computers, computing environment, and physical data centres that it uses in processing of personal data. The audits are performed by independent, third-party auditors according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework. Personal data is stored in the EU according to the application configuration implemented by the EPO. It may, however, be made available to subprocessors in other countries, depending on the requirements for maintenance, support or operation of cloud-hosted services, and the availability of this expertise. If access is granted, it is always temporarily and only to the data required for the specific maintenance, support or operation procedure being carried out. The following safeguards are implemented: • In all transfers to third countries, Microsoft uses EU Standard Contract Clauses for data transfer with its sub-processors. • Microsoft requires subprocessors to join the Microsoft Supplier Security and Privacy Assurance Program. This programme is designed to standardise and strengthen data handling practices, and to ensure that supplier business processes and systems are consistent with those of Microsoft. Specific measures relating to the recording of MS Teams meetings: where a virtual meeting is recorded, participants can limit the processing of their personal data by activating/de-activating their microphone and camera. In addition, where there are legitimate grounds, participants can also ask via the chat feature for the recording to be temporarily suspended so that they can contribute without being recorded.

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 94

Name Vaccination campaigns

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 46 - CIO / BIT, DG4 - 44 - General Administration

Entity Name - Controller (Entities) DG4 - 423 - HR Essential Services

External processors

PDG Health Services

External processors	
Name PDG Health Services	

Helios Privatkliniken GmbH:

External processors	
Name Helios Privatkliniken GmbH:	

Description of the processing

Description • Registration to the vaccination (e.g. flu, Coronavirus) is possible via the online booking tool of the external provider (Helios Privatkliniken GmbH for Munich and Berlin staff and PDG Health Services for The Hague staff) and in Vienna the appointments are scheduled with the EPO external occupational health physician directly
• Vaccination is administered by the external service providers.
• Documents to be filled out before getting the vaccination are the questionnaire on the medical history of the person receiving the vaccine and the consent form.
• These documents are required to ensure safe vaccination and are checked, collected and stored by the medical staff who administered the vaccine.
• Upon request of the vaccinated persons, the medical staff can register the vaccination in their vaccination book
• Vaccination may be offered to family members too
• Data processed by OHS are stored in OHS Cority and/or in secured cupboards.

Data Retention Questionnaires are in paper form and are retained according to the following criteria governed by national provisions (normally 10 years).
The OH Physician in Vienna stores the data for 1 year.

Data stored in the EPO registration tool is deleted after 1 year.

Data stored in OHS common box is deleted after 5 years.

Purpose of Processing The purpose of the processing is to offer vaccination to EPO active staff and their family members in the framework of vaccination campaigns organized by the Office. Vaccination shall happen following the relevant national legislations.

Data subjects and categories of personal data

Employees

Health Data	
Health Data	
Contact Information	
Contact Details	Home Address
Personal Email	Phone Numbers
Family Information	
Children's Names	Parents' Names
Spouse's information	Spouse's name
Personal Identification	
Date of Birth	First Name
Surname	

Externals

Health Data	
Health Data	
Contact Information	

Contact Details	Home Address
Personal Email	Phone Numbers
Personal Identification	
Date of Birth	First Name
Surname	

Recipient of the personal data

Recipients of the data D442 Physical Security is in charge of registering family members entering the EPO building and providing them with a temporary badge.

BIT on the exceptional cases when the EPO registration tool has been used.

The data are not used for any other purposes nor disclosed to any other recipient.

Purpose of sharing

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 95

Name Processing of personal data within the framework of the European and International Cooperation units' tasks, duties and activities

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG0 - 02 - Communication, DG4 - 45 - CTO / BIT, DG4 - 46 - CIO / BIT

Entity Name - Controller (Entities) DG5 - 51 - European and International Affairs

External processors

Microsoft

External processors	
Name Microsoft	

AMEX GBT

External processors	
Name AMEX GBT	

Microsoft

External processors	
Name Microsoft	

Description of the processing

Description Principal Directorate European and International Affairs is responsible for developing relations and the implementation of the co-operation policy with the member states and the extension states, and

promotes the strengthening of the European Patent Network (EPN). Moreover, it maintains the relationships with European Union Intellectual Property Office (EUIPO) and the European Commission.

In addition, the Principal Directorate is in charge of the Office's bilateral relations with non-member states, WIPO and international user associations as well as of the multilateral co-operation with the Trilateral and IP5 offices.

The Principal Directorate is composed of the following units: Regional Desk Member States and Neighbouring Countries, Regional Desk IP5, IOs and Global Users, Regional Desk Americas, Africa and ASEAN, and the External Relations Support Team.

For executing the tasks and duties of the respective units, personal data is processed as follows:

1) In a European Cooperation Database and in an International Cooperation Database and /or sharepoint DB respectively country specific data of the Member States and Non Member States national patent offices (NPO) respectively and additional stakeholders mentioned above, such as country profiles, correspondence, agreements concluded, personal data of EPO's contact persons is stored. The data is based on own research or documents from external sources.

The databases also include personal data of the EPO's contact persons at the respective National Patent Offices (NPOs) and its Heads of Offices, political persons in charge of/responsible for the respective NPO or other persons the Principal Directorate co-operates with from the institutions mentioned above. This data is obtained from the respective NPO and stored upon receipt. Once a contact at the NPO changes, the data of the outgoing person is either destroyed or kept for archival/historic/institutional/accountability reasons, since often the units are requested to give the high management information on contacts which took place and with whom. The same applies with regards to the other institutions mentioned above.

The Databases serve not only as a repository but also as a working DB, i.e. for activities/meetings/trainings/event planning including financial budgeting tied to the Member States and Non Member State's co-operation plans/agreements has been drafted and created therein – these might be linked to a separate area monitored by DG5 Operations for the financial processing of invoices.

The Databases further serve as repository of all types of internal statistical data (e.g. EPOQUE Net, FedReg, EPO monthly reports, templates, minutes etc.) and other background information data necessary and required for the purpose of internal documentation preparation for the bilateral co-operation plans/agreements with the Member States, Non Member States and other institutions and the planning of activities, events, high-level meetings, etc.

The Databases called ECDB and ICDB which in their present structure have more historical archive function for the European and International Cooperation units respectively are stored in Lotus Notes.

2) Working level data (e.g. invitations by email, correspondence with the NPOs and other relevant institutions etc. are stored in MS Teams or in the EPO's Email system.

3) The units liaise with AMEX GBT, to which identification documents (e.g. passport copies) of event participants are sent for the purpose of organising a trip (e.g. airplane ticket, hotel) in the context of organising events.

4) It can occur very seldom that an institution (e.g. WIPO) with which the PD51 has a cooperation agreement, requests a bulk of published

Purpose of Processing Carrying out the official duties of PD 51., The purposes of the processing is to have an up-to-date and accessible database for staff of Dir. European Cooperation and Dir. International Co-operation only, of the Member and Non-Member States' NPOs relevant data respectively, which enable planning and preparation of activities/meetings/trainings/events, internal documentation preparation for the bilateral co-operation plans/agreements, generating statistical data including financial budgeting.

patent data, which PD51 endeavours to provide. The delivery of such data may involve the use of post services.

5) Personal data may be shared internally among EPO departments (e.g. the Principal Directorate Communication) and processed for other compatible purposes. For instance, the contact details of certain data subjects working for stakeholders with whom the EPO cooperate, such as institutions and NPOs, could be part of the lists of invitees for events organised by the EPO or used to send other type communications e.g. season's greetings.

Data Retention Data collected by PD 5.1 European and International Affairs are kept for historical/archival reasons indefinitely, however they are minimized to only what is strictly necessary (name, organisation, position); the rest of the data concerning a data subject such as telephone and email addresses are kept only for as long as the data subject collaborates with thre units of the Principal Directorate.

Financial data of externals such as travel tickets etc will be kept until the end of the audits of the accounting period.

For EPO staff and Contractors, the EPO rules (FinRegs) apply.

Data subjects and categories of personal data

Contractors

Sensory and Electronic Information	
Audio Information	Visual Information
Contact Information	
Contact Details	Emergency Contact Details
Phone Numbers	Working email address
Professional Experience & Affiliations	
CV	Qualifications Certifications
Correspondence	
Personal information provided voluntarily	
Financial	
Bank Account Number	Fund Reservation Requests
Travel & Expense	
Expense Details	Travel Booking Details
Employment Information	
Business Unit Division	Company Entity
Department name and/or number	Language preference (of communication)
Personal Identification	

Full Name	Surname
Nationality	
Education & Skills	
Languages	
Government Identifiers	
Passport Number	

Employees

Sensory and Electronic Information	
Audio Information	Visual Information
Contact Information	
Contact Details	Phone Numbers
Working email address	
Building area and site	
Building area and site	
Professional Experience & Affiliations	
CV	
Correspondence	
Personal information provided voluntarily	
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications
Travel & Expense	
Expense Details	Travel Booking Details
Employment Information	
Department name and/or number	Language preference (of communication)
Office Location	Room Number
Personal Identification	
First Name	Full Name
Gender	Surname

Nationality	
Education & Skills	
Languages	
Government Identifiers	
Passport Number	

Externals

Sensory and Electronic Information	
Audio Information	Visual Information
Contact Information	
Contact Details	Emergency Contact Details
Phone Numbers	Working email address
Professional Experience & Affiliations	
CV	
Correspondence	
Personal information provided voluntarily	
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications
Financial	
Bank Account Information	Bank Account Number
Fund Reservation Requests	
Travel & Expense	
Expense Details	Travel Booking Details
Employment Information	
Business Unit Division	Company Entity
Job Title Role	Language preference (of communication)
Office Location	
Personal Identification	
First Name	Full Name

Gender	Surname
Nationality	
Education & Skills	
Languages	
Government Identifiers	
Passport Number	

Recipient of the personal data

Recipients of the data Personal data are only shared on a need to know basis, as follows:
· EPO staff from PD 5.1 – access to personal data related to European and International cooperation;
· Staff from the hierarchical line of the units and PD5.1
· Staff from the Presidential Office;
· EPO staff from all the units involved in the meetings (BIT, Protocol, Communication);
· Microsoft staff;
· Amex GBT staff;
. Physical security (entry controls) responsibility of DG 4
. National patent offices, international organisations and other organisations and associations with which PD51 have agreement with.

Purpose of sharing Personal data are only shared on a need to know basis for the following purposes:
· EPO staff from PD 5.1 – carrying out duties of cooperation;
· Staff from the hierarchical line of PD 5.1 - internal briefings of top management;
· Staff from the Presidential Office - internal briefings of the President;
· EPO staff from all the units involved in the meetings (BIT, Protocol, Communication): arranging for missions, organisation of meetings;
· Microsoft and BIT staff: providing Microsoft services and support;
· Amex GBT staff: for providing the services;
. Physical security for entrance/access controls
. National patent offices, international organisations and other organisations and associations with which PD51 have agreement with - for exchange of information and organising meetings in the scope of a cooperation agreements and very rarely for sending published patent data

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation In case of international co-operation, to Patent Offices outside the EPC contracting states and to international organisations (e.g. WIPO)

Transfer mechanism(s) The recipient provided appropriate safeguards, Derogation in accordance with Art. 10 DPR

Country where data might be transferred - Processor (Vendors) Microsoft - United States, AMEX GBT - Netherlands

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, International cooperation activities, Public Authorities/Government Bodies, Organisation of an event

Derogations Art. 10 DPR The transfer is necessary for the performance of a task in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning, or to perform obligations arising from its duty of co-operation with the contracting states

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 96

Name House Ban List

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 44 - General Administration

Entity Name - Controller (Entities) DG4 - 44 - General Administration

External processors

Apleona Vienna

External processors	
Name Apleona Vienna	

Kötter

External processors	
Name Kötter	

G4S

External processors	
Name G4S	

Securitas

External processors	
Name Securitas	

Description of the processing

Description Personal data is processed according to Art. 3 of Circular 380 , for the purpose of implementing the necessary access control measures for the protection of the EPO staff and their visitors, its information and assets. Persons are banned access to the Office whenever they may entail a risk for their staff, visitors, information or assets.

Data Retention All categories of personal data of the individual are immediately removed from the list as soon as Operations Office has been informed by PD 42 that the house ban has been lifted. It is expected that PD 42 informs Operations Office/security as soon as any of the house ban is lifted to act accordingly.

Purpose of Processing Personal data is processed according to Art. 3 of Circular 380 , for the purpose of implementing the necessary access control measures for the protection of the EPO staff and their visitors, its information and assets. Persons are banned access to the Office whenever they may entail a risk for their staff, visitors, information or assets.

Data subjects and categories of personal data

Employees

Employment Information	
Personnel Number	
Personal Identification	
Full Name	

Externals

Personal Identification	
Full Name	

Recipient of the personal data

Recipients of the data EPO Operations office staff members and security contractors staff at all sites.

PD 42/HR Business Partners and HR Interlocutors for updates or controls of data accuracy.

Purpose of sharing Need to know basis to perform the duties.

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 103

Name Processing of personal data within the framework of approval of formal documentation by the President's Office

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG0 - 01 - President`s Office - Vice-President

External processors

OpenText

External processors	
Name OpenText	

Description of the processing

Description In the frame of the submission for information or approval process by the President, both referred to as "Note to the President" or "NttP", the President's Office (PO) is entrusted to receive and process, via the CommonLog tool, formal documents and requests submitted by all relevant departments throughout the EPO.

Data Retention The files are subject to an administration retention Time, which corresponds to the President's term of office. At the end of the President's term of office, all files are transferred to the EPO archives (for permanent preservation, including the personal data concerned).

Purpose of Processing Administrative handling of Notes to the President (NttP) provided by EPO departments to inform or request approval of the President of the Office

Data subjects and categories of personal data

Employees

Health Data	
Health Data	

Contact Information	
Contact Details	
Professional Experience & Affiliations	
Qualifications Certifications	
Correspondence	
Additional Information which might be provided in the course of exchanges	
Background Checks	
Criminal Records	Reference or Background Checks
Employment Information	
Appeals Records Information	Benefits and Entitlements Data
Business Unit Division	Company Entity
Contract Type	Disciplinary Action
End Date and Reason for Termination	Exit Interview and Comments
Grade	Grievances and Complaints
Job Application Details	Job Title Role
Line Reporting Manager	Office Location
Performance Rating	Personnel Number
Previous Work History	Rewards history
Start Date	
Personal Identification	
Age	Date of Birth
Disability or Specific Condition	First Name
Full Name	Gender
Surname	Marital Status
Nationality	
Education & Skills	
Academic Transcripts	Education and Training History

Educational Degrees	Languages

Prospective Employees

Health Data	
Health Data	
Contact Information	
Contact Details	Personal Email
Phone Numbers	
Professional Experience & Affiliations	
Professional Memberships	Qualifications Certifications
Background Checks	
Criminal Records	Reference or Background Checks
Employment Information	
Contract Type	Job Application Details
Job Title Role	Military Status
Previous Work History	Start Date
Personal Identification	
Age	Date of Birth
First Name	Full Name
Gender	Surname
Marital Status	Nationality
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages

Former Employees

Contact Information	
Contact Details	Personal Email
Employment Information	
Appeals Records Information	Company Entity

End Date and Reason for Termination	Personnel Number
Previous Work History	
Personal Identification	
Age	Date of Birth
First Name	Full Name
Gender	Surname
Marital Status	Nationality

Externals

Contact Information	
Contact Details	Personal Email
Phone Numbers	
Professional Experience & Affiliations	
Political Affiliation and Activities	Professional Memberships
Qualifications Certifications	
Employment Information	
Company Entity	Job Title Role
Personal Identification	
First Name	Full Name
Nationality	

Recipient of the personal data

Recipients of the data The NttP (and accompanying documents) containing all the types of personal data (of staff and/or externals) is submitted together with the personal data of the responsible sender(s) to the President via the Common Log. Before reaching the President, the NttP is usually subject to a consultation process which make the data accessible for comments, contributions and/or pre-approval by relevant stakeholders in the EPO and staff working in the PO on a need to know basis.

Purpose of sharing

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Country where data might be transferred - Processor (Vendors)
OpenText - United Kingdom

Reasons for the transfer

Transfer mechanism(s)	Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures	EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 120

Name Study on European Patent Applications to produce statistics on the gender of inventors.

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG0 - 032 - Chief Economist

External processors

External consultants for CEU

External processors	
Name External consultants for CEU	

Description of the processing

Description The study is organised by the EPO to produce statistics on the gender of inventors listed in European patent applications. While most of the study is based on EPO's public database PATSTAT, this database does not yet include complete data on patent applications filed with EPO as of 2020

In order to also enable the production of gender statistics as of 2020, the EPO will provide the contractors with a dataset extracted from EPASYS including the name, surname, and country of residence as well as a randomly generated identifier for all inventors of European patent applications filed at the EPO as of 2020.

Using this dataset, the contractors will use a predefined algorithm to attribute a gender to these inventors. As a next step they will delete the personal data (names, surnames and country of residence) from the dataset before sending it back to the EPO.

The dataset with gender data will then be matched by the EPO with the respective patent applications. EPO will then use the matched dataset to produce a statistical analysis of the share of women among inventors of inventions for which patent applications were filed at the EPO as of 2020.

The final report without reference to individual personal data will be published e.g. the data will be used to report, in the context of the Patent Index, on the gender of inventors (using an algorithmically-attributed gender) listed in European patent applications.

Data Retention The personal data (names, surnames and country of residence) received and processed by the contractors will be deleted by the contractors prior to sending back to EPO the results of the algorithmic gender attribution.

The gender data and statistics will be kept by CBA and the CEU data stored in CBA database is kept for the maximum period of 12 months after the study and then deleted.

Purpose of Processing Reporting of statistics, in the context of the Patent Index, on the gender of inventors (using an algorithmically-attributed gender) listed in European patent applications., Statistical study on the gender of inventors listed in European patent applications.

Data subjects and categories of personal data

Externals

Employment Information	
Office Location	
Personal Identification	
Full Name	Gender

Recipient of the personal data

Recipients of the data N/A

Purpose of sharing

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures.

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 122

Name Learning Management System

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 46 - CIO / BIT

Entity Name - Controller (Entities) DG4 - 421 - Talent Acquisition and Development

External processors

SAP

External processors	
Name SAP	

Description of the processing

Description EPO Talent Academy uses internal systems, external online learning platforms and any other service provider for talent development activities. These systems and platforms process personal data of staff members.

A digital platform known internally as iLearn (and built on SAP SuccessFactors technology), facilitates the management of the talent development activities of the employees, creating the learning catalogue (trainings, e-learning, coachings which could be provided by external contractors whom will have access to data if the case may be), promoting courses, events, collecting the learning history of the employees, evaluating quality and effectiveness of the services for the continuous improvement and development of the learning activities. iLearn is, consequently, the Learning Management System for the organisation.

iLearn makes the above possible as portal for any employee to access information on diverse learning resources and provides access to the external online learning platforms (LinkedIn Learning, Udemy for Business, Coursera, Udacity). A dedicated record of processing activities covering these online external learning platforms is available.

Personal data are processed for the following purposes:

• To plan and organise training activities.
• To create a training history log for EPO staff.
• To issue certificates of participation for the different training courses.
• To collect feedback from participants so that the EPO Talent development teams (4212 and 4213) can deliver better and more effective development activities, according to staff needs and knowledge as well as the skills necessary for their job.
• To evaluate via quizzes, confidence surveys and assessments, the ability of participants to apply the new skills learnt in the development activities.
• To keep logs that include user activity (access time, actions, etc.), which could be used to resolve user incidents.
• Personal data is sometimes collected to create user accounts for online learning platforms or made available to service providers of talent development activities for organisational purposes.

Data Retention Any personal learning information will be kept during the period of active employment of the employee.

EPO Talent Development teams will use course completion data for reporting on talent development activities. This information will be retained for 5 years. Service providers will be instructed to delete the data retained related to usage by EPO staff member on finalisation of the relationship with the EPO.

Purpose of Processing To issue certificates of participation for the different training courses., To plan and organise training activities., To keep logs that include user activity (access time, actions, etc.), which could be used to resolve user incidents., To collect feedback from participants so that the EPO Talent Academy can deliver better and more effective development activities, according to staff needs and knowledge as well as the skills necessary for their job., To evaluate via quizzes, confidence surveys and assessments, the ability of participants to apply the new skills learnt in the development activities., Personal data is sometimes collected to create user accounts for online learning platforms or made available to service providers of talent development activities for organisational purposes., To create a training history log for EPO staff.

Data subjects and categories of personal data

Employees

General	
Personal Information in SAP	
Contact Information	
Contact Details	Working email address
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data

IDP	Instructor related data
Learning external events	Learning history
Learning plan	Ratings
Social learning inputs	
Examination content data	
Examination marks	Examination result
Employment Information	
Business Unit Division	Department name and/or number
Grade	Job Group
Job Title Role	Language preference (of communication)
Personal Identification	
First Name	Full Name
Surname	
Education & Skills	
Education and Training History	

Externals

Contact Information	
Contact Details	

Recipient of the personal data

Recipients of the data Personal data are disclosed to the following recipients:

- EPO Talent Development teams staff involved in the administration of talent development activities has access to the personal data of all EPO staff members that is available via SuccessFactors LMS
- iLearn administrator in EPO Talent Development teams: Creation, administration and maintenance of basic learning elements (courses offered, development programmes, catalogues, assignment profiles), creation and editing of surveys, recording learning events, assignment and registration of staff to courses, creation of content in the system, creation and access to learning reports, allocation of coach to coachee, visualising staff member's learning history
- Line managers have access to the learning history of their direct reportees via reporting functionalities in iLearn (including all mandatory online learning courses, e.g. those that are part of a staff member development plan) to support the staff member's professional development
- Instructor: View list of courses authorised to teach, view lists of past and upcoming learning events where the instructor is involved, view list of participants to his/her learning events, record attendance to his/her learning events
- Learning Consultant & HRBP: View information about staff enrolment and progression within a development programme, view learning history for staff members, view external requests (participation to an external conference)
- BIT Department, as an internal processor in the role of application manager, has access to the data in iLearn - To support line managers and staff with regard to professional development
- Coach: View list of past and future assigned learning events for coachee, see results of coachee's assessments, complete coachee's version of confidence survey to provide effective coaching
- MST company, Munich (Germany) - External company that provides SF Learning administration as part of the EPO externalisation project
- Service providers of training activities, including companies that support the EPO Talent Development teams in the administration of learning activities, as well as companies that provide access to their online learning platforms as part of a contractual relationship with the EPO have access to personal data on a strictly need-to-know basis.

Purpose of sharing EPO Talent Academy - For administration purposes.
Line Managers - To support personal development of their staff-
EPO BIT Department - In the role of application manager.
Instructors, coaches - To provide the service
Learning consultants and HRBPs - to support them in their functions
MST - To provide the service

Service Providers of training services - To provide the service
Online external learning platforms - To provide the service

Transfer

Transfer No

Country where data might be transferred - Processor (Vendors) SAP - Germany

Transfer to public authority and/or International Organisation

Reasons for the transfer

Transfer mechanism(s)

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 125

Name Fitness & Vitality Service

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 44 - General Administration

Entity Name - Controller (Entities) DG4 - 422 - People Engagement and Partnership

External processors

High Five Health Promotion B.V

External processors	
Name High Five Health Promotion B.V	

Description of the processing

Description Steps of the Procedure

In order to use the fitness services provided by High Five, the staff member has first to register in the High Five portal (using the High Five Connect application) and become a member.
There are two kind of services.

1. Fitness services provided at the EPO premises
This service is for all staff assigned to Munich Isar and PH buildings and The Hague buildings.

1.1. Users of the fitness services are required to undertake an induction training with the High Five trainer scheduling an appointment via the booking tool.
1.2. During the induction training, users are also introduced with the functionalities of the High Five Connect application a hub where users can manage memberships, schedule bookings, track progress, join the health & wellbeing community and maintain contact with High Five professionals
1.3. The only personal information of the users that High Five shares with the EPO is the list with the names of the members. This list is regularly sent by High Five to the EPO Security Services in order to manage the access rights to the fitness rooms via the EPO personal badge.

1.4. The Security Services and High Five will provide Health and Safety department with anonymous aggregated data on the usage of the service.
1.5. Services that are free of charge
As long as corona measures are maintained: online courses and online one-to-one consultations with a fitness expert
Use of the on-site gyms in Munich (Isar and PschorrHöfe) and in The Hague, induction by the fitness trainer
Via High Five Connect app: online courses, fitness consultations, fitness community, online training plans
1.6. Services that are not free of charge
On-site classes, personal trainer, physiotherapy, lifestyle coaching
1.7. If you leave the Office or if you decide to cancel your subscription, please contact High Five (fitnessepo@highfive.fit).

2. Membership at external fitness clubs
This service is for staff assigned to Munich Haar building, Berlin, Vienna and Brussels.
2.1. Membership is only possible in external fitness clubs that have been agreed between EPO and High Five (see the list in the dedicated intranet page of the Health & Safety department)
2.2. When staff register for this service in the online tool, they are automatically informed that their name will be shared with the fitness club and the Health and Safety department for auditing reasons
2.3. High Five share the names of registered staff with the external fitness club for membership and invoice purposes.
2.4. High Five share the names of registered staff with Health & Safety department for audit and invoice purposes.
2.5. Services that are free of charge
As long as corona measures are maintained: online courses and online one-to-one consultations with a fitness expert
Fitness membership in external local gyms
Via High Five Connect app: online courses, fitness consultations, fitness community, online training plans
2.6. Services that are not free of charge
Check-up, personal trainer, beverages, supplements, massages
2.7. As the High Five and the external local gyms run totally cashless, when registering, you may be asked to provide your back account. You will be charged only if you book/buy services/products not covered by your membership or if you benefit, as family member, external or retired staff from discounted rates.
2.8 If you leave the Office or if you decide to cancel your subscription, please contact High Five (fitnessepo@highfive.fit). Cancellation from external gyms has to be communicated to High Five one month in advance.

Data subjects are:
- Employees, Contract agents and their family members
- Pan-European Seal Program trainees

The following data types may be processed.
A) Data accessible by EPO and the external service provider
• Identity data – Name, Date of birth, Gender, personal ID number, place of work
• Contact data – work place, E-mail address, Phone number
B) Data accessible by the external service provider only
• Activity data – Visit history, bookings, training schedule
• Payment data – Banking details, payment history, invoices
• Health data – Weight, Blood pressure, Height, Pre-existing conditions, Information regarding nutrition

Purpose of Processing The EPO commits to provide its staff members with services that are directed at maintaining a healthy lifestyle. This service targets the physical and mental health of all our staff members and provides a space where healthy habits can be encouraged by professional staff of the external providers.

Data Retention Processes are set up to guarantee the following retention periods:

- In Virtuagym – HighFive Connect member data will remain until manually deleted by High Five or 1 year after cancelation of the contract if the account is no longer in use
- Due to tax legislation High Five will need to store payment data (invoices) for a period of maximum 7 years
- In Technogym Wellness Cloud, the data will be kept for 12 months after membership cancelation. Processes will be set up to guarantee these retention times.

Data subjects and categories of personal data

Former Employees

Contact Information	
Contact Details	Working email address
Personal Identification	
Full Name	

Externals

Personal Identification	
Full Name	

Recipient of the personal data

Recipients of the data The recipients of data are:
1. High Five Health Promotion B.V and sub-processors
2. Facility Management- Security
3. Health & Safety department

Health & Safety may have access to aggregated data on the use of the service.

The data are not used for any other purposes nor disclosed to any other recipient.

The external fitness gyms receive the personal data in their role of data controllers of the employee's personal data for all the services they provide.

Purpose of sharing Processor: High Five Health Promotion B.V

Sub-processors:
- Technogym S.P.A (Italy) for training data (Biocircuit training data).
- Digifit B.V (Netherlands) (publisher of Virtuagym) for administration, booking, member portal tool and back-up.
- Hestronic (Netherlands) for IT support.
- Severius (Netherlands) for Hosting
- Microsoft (Netherlands) for Communications with members.

Internal processors:
- Health & Safety department for auditing purposes (check that the persons applying for membership in the external fitness club are EPO staff members)
- Facility Management-Security for the management of the access rights to the fitness rooms via the EPO personal badge.

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 126

Name EP Full Text for Text Analytics

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 46 - CIO / BIT, DG4 - 45 - CTO / BIT

Entity Name - Controller (Entities) DG5 - 54 - Patent Intelligence

External processors

Microsoft

External processors	
Name Microsoft	

Google

External processors	
Name Google	

Microsoft

External processors	
Name Microsoft	

Google Cloud Platform

External processors

Name	
Google Cloud Platform	

Description of the processing

Description The European Patent Office (EPO) distributes a bulk data set consisting of titles, abstracts, descriptions, claims and search reports of EP publications that is based on input data which is collected from the Patent Grant Procedure. The collected input data is used to create reformatted, and repackaged data sets for public distribution. This data is in text format potentially addressing specific user categories who wish to conveniently load the data into their own systems.

The packaged data is made available to the public via the Google Cloud platform.

The cloud platform provider makes service usage data available to the EPO. This service usage data can be analysed within the EPO or using the cloud service provider supplied tools. Data are not anonymised when used for interaction with users for support and service delivery management relating to service usage.

Data Retention The EP publications are public data, therefore the data not deleted.
User data is retained for up to 7 years after it can be reasonably expected that there is no immediate operational need anymore.

Purpose of Processing Distribution of the EP data to the public intended for text analytics, Analytics and ensuring correct service functioning

Data subjects and categories of personal data

Externals

Network/application Interaction Data	
Session content	Session details
Session metadata	
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications
Browsing Information	
Browser type	Browsing Time
Cookie Information	IP Address
Network Interaction History	Website History
User Account Information	
Account Number	Third-party User Identifier
User ID	

Employees

Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications
User Account Information	
User ID	

Former Employees

Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications

Recipient of the personal data

Recipients of the data The patent record content can be made available to anyone who uses the service. These users may be world wide.

Where necessary to perform its tasks, non-patent personal data may be shared on a need-to-know basis with staff undertaking duties in the following areas of the EPO: Patent Intelligence, BIT, DG1 and senior EPO management (EPO Observatory, VP5 Office, President Office, CGS, MAC), and Google as external processor.

Purpose of sharing

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation The published data are publicly accessible.

Transfer mechanism(s) Data Protection EU Comm Standard Contractual Clauses, Derogation in accordance with Art. 10 DPR

Country where data might be transferred - Processor (Vendors)
Microsoft - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, The patent record content is made available to anyone world-wide.

Derogations Art. 10 DPR The transfer is made from a register which, according to the legal provisions of the European Patent Organisation, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down for such consultation are fulfilled in the particular case

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 127

Name Open Patent Services

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 45 - CTO / BIT, DG4 - 46 - CIO / BIT

Entity Name - Controller (Entities) DG5 - 54 - Patent Intelligence

External processors

Pantheon| European Patent Office | Technology

External processors	
Name Pantheon| European Patent Office | Technology	

Microsoft

External processors	
Name Microsoft	

Pantheon | European Patent Office | Unknown

External processors	
Name Pantheon | European Patent Office | Unknown	

Google Ireland Limited

External processors

Name
Google Ireland Limited

Google Ireland Limited

External processors
Name
Google Ireland Limited

Microsoft

External processors
Name
Microsoft

Description of the processing

Description The European Patent Office (EPO) provides Open Patent Services (OPS) which is a web service that provides access to the EPO's patent data collections.

The data made available via the OPS service is extracted from the EPO's patent procedure related information collections and the EPO's world-wide patent related data collections and databases.

Registered users are granted free access to a specific volume of data up to a certain ceiling defined in the OPS terms and conditions.

Registered users willing to pay for more substantial volumes of data can record billing contact details and apply for access to higher volumes of data in the form of a yearly subscription.

The subscription and payment are in scope of the record Patent Knowledge Webshop.

Users may also be contacted for service delivery (support) related issues.

Additional end user information is collected for analytics purposes in order to ensure efficient delivery of the service.

Data Retention User data is retained for up to 7 years after it can be reasonably expected that there is no immediate operational need anymore (e.g. cancellation of a subscription).
Technical service access data can be retained for up to 7 years in order to analyse usage patterns.
Information contained in the patent records is public data which is never deleted.

Purpose of Processing Usage analytics., Communication with users., Access management., Deliver access to OPS.

Data subjects and categories of personal data

Externals

General
Any other information
Network/application Interaction Data

Session content	Session details
Session metadata	
Contact Information	
Contact Details	Country
Mobile Phone Number	Phone Numbers
Private Phone Number	Working email address
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications
Employment Information	
Company Entity	Department name and/or number
Job Title Role	Office Location
Browsing Information	
Browser type	Browsing Time
Cookie Information	IP Address
Network Interaction History	Website History
Personal Identification	
Digital signature	First Name
Full Name	Gender
Surname	
User Account Information	
Account Age	Account Number
Account Password	User ID

Employees

Contact Information

Contact Details	Country
Phone Numbers	Working email address
Correspondence	
Additional Information which might be provided in the course of exchanges	Personal information provided voluntarily
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications
Employment Information	
Company Entity	Department name and/or number
Job Title Role	
Personal Identification	
First Name	Full Name
Surname	

Former Employees

Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications

Recipient of the personal data

Recipients of the data The patent record content can be made available to anyone who uses the service. These users may be world-wide.

Where necessary to perform its tasks, non-patent personal data may be shared on a need-to-know basis with staff undertaking duties in the following areas of the EPO: Patent Intelligence, BIT, DG1, and senior EPO management (VP5 Office, President Office, CGS, MAC). Third-party service providers for provision of the service as well as maintenance and support purposes.

Purpose of sharing

Transfer

Transfer Yes

Country where data might be transferred - Processor (Vendors)
Google Ireland Limited - Hong Kong, Google Ireland Limited - Taiwan, Google Ireland Limited - Brazil, Google Ireland Limited - Qatar, Google Ireland Limited - Indonesia, Google Ireland Limited - Singapore, Google Ireland Limited - Malaysia, Google Ireland Limited - Saudi Arabia, Google Ireland Limited - United States, Google Ireland Limited - Philippines, Google Ireland Limited - India, Google Ireland Limited - Australia, Google Ireland Limited - Chile, Microsoft - United States

Transfer to public authority and/or International Organisation
Published patent data are distributed to the public world-wide.

Transfer mechanism(s) The recipient provided appropriate safeguards, Derogation in accordance with Art. 10 DPR

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, The service is intended to deliver patent data to world-wide users.

Derogations Art. 10 DPR The transfer is made from a register which, according to the legal provisions of the European Patent Organisation, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down for such consultation are fulfilled in the particular case, The transfer is necessary for the performance of a task in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning, or to perform obligations arising from its duty of co-operation with the contracting states

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 129

Name Post grant contact management

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG4 - 41 - Finance

External processors

Microsoft

External processors	
Name Microsoft	

Microsoft

External processors	
Name Microsoft	

Description of the processing

Description A list of contact persons at national patent offices in Contracting States are maintained for the purpose of administering Postgrant Validations team activities and communication with respect to monitoring Article 39 EPC – Payments by the Contracting States in respect of renewal fees for European patents.

The National Patent Office contact persons provide EPO with their contact details.

The contact list is stored on EPO internal storage systems and the communication is carried out using MS Outlook, in the PostGrant@epo.org shared mailbox.

Only patent numbers are used to identify patents during the communication.

Data Retention Contact details are kept for the time being in the respective function at a National Office. If considered appropriate, it is also deleted if it can reasonably be expected that there is no operational need anymore. The personal data will be erased at the very latest 3 years after somebody has left the respective function at a National Office

Purpose of Processing Communication with contacts from national patent offices in contracting states with respect to monitoring Article 39 EPC

Data subjects and categories of personal data

Employees

Contact Information	
Contact Details	Phone Numbers
Working email address	
Employment Information	
Job Title Role	
Personal Identification	
First Name	Full Name
Surname	

Externals

Contact Information	
Contact Details	Phone Numbers
Working email address	
Employment Information	
Job Title Role	
Personal Identification	
First Name	Full Name

Surname	

Recipient of the personal data

Recipients of the data Personal data are only shared with other EPO departments (IT Cooperation, Legal Services, Member states and neighbouring countries Finance undertaking relevant activities.

Purpose of sharing Personal data are shared in order to contact the designated representatives within the National Patent Offices in contracting states with respect to monitoring Article 39 EPC.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) Data Protection EU Comm Standard Contractual Clauses

Country where data might be transferred - Processor (Vendors) Microsoft - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 134

Name Official Publications

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 46 - CIO / BIT, DG4 - 45 - CTO / BIT

Entity Name - Controller (Entities) DG5 - 54 - Patent Intelligence

External processors

Arcanum

External processors	
Name Arcanum	

Not Applicable

External processors	
Name Not Applicable	

Description of the processing

Description The European Patent Office (EPO) has processes for collating and assembling various publications required or closely related to the European Patent Convention, including:

- The Official Journal - source of official information and general notices from the EPO, and of other information relevant to the EPC or its implementation.

- EP Bulletin - regular EPO publication containing bibliographic data, as well as data concerning the legal status of European patent applications and patents.

- Legal Texts: e.g. European Patent Convention

- EP Patent documents (A & B)

- EP Register - the most complete and up-to-date source of publicly available procedural information on European patent applications as they pass through each stage of the granting process. Unitary Patent process related information is also included.

- EP file inspection - the files relating to European patent applications and granted patents, and to international applications under the PCT for which the European Patent Office acts as a designated or elected Office, are available for inspection online, free of charge, via the European Patent Register. Unitary Patent process related information is also included.

Personal information of the EPO staff involved in the preparation and processing of content is processed.

Data Retention Information contained in the patent records, and other publications covered by this record, is public data which is never deleted.

Purpose of Processing Preparation of Official publication content., Making Official publication content available to the public.

Data subjects and categories of personal data

Externals

General	
Input provided during the deliberation and decision-making process	
European Patent Register Data	
Data provided by the data subjects	
Correspondence	
Additional Information which might be provided in the course of exchanges	Personal information provided voluntarily
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications

Employees

Patent Process Related Data

Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications
Personal Identification	
Full Name	

Former Employees

Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications

Recipient of the personal data

Recipients of the data The patent record content can be made available to anyone who uses the service. These users may be world-wide.

Where necessary to perform its tasks, non-patent personal data may be shared on a need-to-know basis with staff undertaking duties in the following areas of the EPO: Patent Intelligence, BIT, DG1, EPO Legal Services, EPO Boards of Appeal, Observatory on Patents and Technology and senior EPO management (VP5 Office, President Office, Corporate Governance Service (CGS), MAC.)

Purpose of sharing The legal text data are shared with DG1 to upload into their Single Legal Source (SLS) tool.

The source data for Bulletin processing are shared with Patent Intelligence for their own processing requirements (e.g. Bulletin Search, Bulk data products).

Otherwise for reporting and administration of EPO activities.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation The published patent data are publicly accessible.

Transfer mechanism(s) Derogation in accordance with Art. 10 DPR

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer The service is intended to prepare and distribute data to world-wide public users.

Derogations Art. 10 DPR The transfer is made from a register which, according to the legal provisions of the European Patent Organisation, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down for such consultation are fulfilled in the particular case

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 137

Name Federated Services

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 46 - CIO / BIT, DG4 - 45 - CTO / BIT

Entity Name - Controller (Entities) DG5 - 54 - Patent Intelligence

External processors

Not Applicable

External processors	
Name Not Applicable	

Description of the processing

Description The European Patent Office (EPO) offer services to end users that combine inputs collected from distributed patent process related sources (e.g. National Patent Offices) into a combined view. This record relates only to the processing done by the EPO after receipt of data from the distributed sources.

The services concerned include:

- Global Dossier - single-point access to dossier content (file inspection) of patent documents from numerous intellectual property offices, including the IP5 offices. The file content and their translations are made available to the EPO by Global Dossier partner offices.

- Federated Register - single point of access to post-grant bibliographic and legal status information on European patents. It is available free of charge.

Additional end user information is collected for providing alerts and for analytics purposes in order to ensure efficient delivery of the service.

Purpose of Processing Analytics and managing service delivery., Combining patent process related information from multiple patent offices into a single representation.

Data Retention User data is retained for up to 7 years after it can be reasonably expected that there is no immediate operational need anymore (e.g. cancellation of a subscription).
Technical service access data can be retained for up to 7 years in order to analyse usage patterns.
Information contained in the patent records is public data which is never deleted.

Data subjects and categories of personal data

Employees

Network/application Interaction Data	
Session content	Session details
Session metadata	
Contact Information	
Contact Details	Country
Personal Email	Phone Numbers
Working email address	
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications
Employment Information	
Company Entity	Language preference (of communication)
Browsing Information	
Browser type	Browsing Time
Cookie Information	IP Address
Network Interaction History	Website History
Personal Identification	
First Name	Surname
User Account Information	
Account Age	Account Number
Account Password	User ID

Externals

Network/application Interaction Data

Session content	Session details
Session metadata	
Contact Information	
Contact Details	Country
Personal Email	Phone Numbers
Working email address	
Correspondence	
Personal information provided voluntarily	
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications
Employment Information	
Company Entity	Language preference (of communication)
Browsing Information	
Browser type	Browsing Time
Cookie Information	IP Address
Network Interaction History	Website History
Personal Identification	
First Name	Surname
User Account Information	
Account Age	Account Number
Account Password	User ID

Former Employees

Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications

Recipient of the personal data

Recipients of the data The patent record content can be made available to anyone who uses the service. These users may be world wide.

Where necessary to perform its tasks, non-patent personal data may be shared on a need-to-know basis with staff undertaking duties in the following areas of the EPO: Patent Intelligence, BIT, DG1 and senior EPO management (Observatory on Patents and Technology, VP5 Office, President Office, CGS, MAC).

Purpose of sharing

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation The published data are publicly accessible.

Transfer mechanism(s) Derogation in accordance with Art. 10 DPR

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer Public access to service content.

Derogations Art. 10 DPR The transfer is made from a register which, according to the legal provisions of the European Patent Organisation, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down for such consultation are fulfilled in the particular case

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 144

Name Automated Number Plate Recognition (ANPR) system

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 44 - General Administration

Entity Name - Controller (Entities) DG4 - 44 - General Administration

External processors

Security and Reception Services Contractor at all EPO sites

External processors	
Name Security and Reception Services Contractor at all EPO sites	

Public authorities in The Hague

External processors	
Name Public authorities in The Hague	

NSecure

External processors	
Name NSecure	

Description of the processing

Description The ANPR system registers the number plates of visitors, staff members and contractors vehicles having access to the EPO premises, reading the badge presented to the access control reader, assigning the number plate captured by ANPR cameras deployed at parking entrances to the badge holder registry in the EPO access control system AEOS.

This is done without directly identifying the holder of the badge (if someone presents the badge of another person, the number plate of the vehicle will get assigned to the badge holder as an additional identified, the same as another badge number but in this case a number plate of a vehicle). This limitation is known and accepted by Operations Office.

Data Retention Access Logs: 1 year, in line with the retention period of the access control logs registered under the Access Control System.
Badge number and vehicle number plate: For the validity of the badge until that one is withdrawn.

Purpose of Processing Personal data is processed for the purpose of managing the limited number of parking places available at EPO as well as it usage policy. Vehicle drivers will be identified by Security to be informed in cases of non-compliance with parking rules, works requiring their vehicles to be moved or circumstances in which the communication to the vehicle owner will facilitate the management of the parking areas and its limited space. To identify the driver of the vehicle, Security will access the entry logs in the access control system related to the number plate, this is done for cases in which the owner needs to be contacted by security to remove the vehicle or in similar situations. Additionally, in coordination with the EPO Safety Expert, identify vehicles' owners in case of severe unsafe driving behaviour on the premises. The vehicle drivers will be identified by accessing the Access Control System AEOS and verifying the badge to which the number plate is linked, in general the person presenting the badge will correspond to the driver of the vehicle. In connection with the Access Control System, an automated report containing anonymous statistical data regarding the number of vehicles accessing the parking facilities is sent to Directorate Planning. The data is collected to facilitate the analysis of CO2 emissions that is later published as a KPI on the EPO intranet.

Data subjects and categories of personal data

Contractors

General	
Any other information	
Contact Information	
Working email address	
Correspondence	
Any other information	
Personal Identification	
First Name	Full Name

Employees

General	
Any other information	
Sensory and Electronic Information	
Visual Information	
Contact Information	

Working email address	
Correspondence	
Any other information	
Employment Information	
Personnel Number	
Personal Identification	
First Name	Full Name

Externals

General	
Any other information	
Correspondence	
Any other information	
Personal Identification	
Full Name	

Recipient of the personal data

Recipients of the data Personal data registered in AEOS is accessible to those organisational units working in security or reception services during the retention period established and for the performance of their duties (monitoring parking usage, informing users about the violation of parking rules, if required to have their vehicles moved in case of works or other similar situations), or by the Safety Expert in case of severe unsafe behaviour.

The EPO Building Maintenance Team experts and technicians and the external maintenance company technicians have access to the application and its hardware for the performance of the maintenance of those ones.

In connection with the Access Control System, an automated report containing the number of vehicles accessing the EPO parking facilities is sent to Directorat Planning via Access Control System, this report does not contain though any individual personal data but statistical figures.

Purpose of sharing The data is only used internally by Operations Office staff and its external security contractor staff. If other recipients (e.g. Ethics and Compliance, Police, Safety Expert) request the information this will be individually asked to the Delegated Controller.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation In case of criminal offenses, data are transferred to national authorities such as the Police, the Tribunal in The Hague in line with EPO site agreement.

Transfer mechanism(s) Legally binding and enforceable instrument between public authorities or bodies

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer Public Authorities/Government Bodies

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 145

Name Video Surveillance Systems

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 44 - General Administration

Entity Name - Controller (Entities) DG4 - 44 - General Administration

External processors

Insurance companies

External processors	
Name Insurance companies	

National authorities

External processors	
Name National authorities	

Kötter

External processors	
Name Kötter	

G4S

External processors	
Name G4S	

Securitas

External processors	
Name Securitas	

Maintenance company in charge of the service of the application

External processors	
Name Maintenance company in charge of the service of the application	

Description of the processing

Description The EPO operates a Video Surveillance System (VSS) at its sites of Munich, The Hague, Vienna and Berlin. The VSS is composed of video surveillance cameras and a hardware infrastructure of other elements such as cabling, database storage for images, monitoring and analytics software and control equipment.

The VSS collects images of data subjects entering/leaving/walking in given areas of the EPO premises, car parking, including an Automatic Number Plate Recognition (ANPR), data subjects and cars inside the premises in parking areas hallways.

The cameras record digital images indicating time, date and location. The VSS also collects metadata from the images captured by the system (e.g. motion, direction, time, speed). Metadata embedded in the images is used to initiate alarms based on specific triggers and it is also stored in parallel and for the same retention time in order to recognise visual security breaches, optimising the use of the system to detect for example abandoned packages or suspicious movement, movement in directions that are unusual or erratic. This serves to trigger automated alerts in the system and diminish the intervention time of the security officers. Metadata serves also to perform faster searches in stored images without the need to spend large amounts of time looking at the images.

The EPO has established a security-zoning model in which areas have been delimited based on the security risks that they face and the safety processes that they support. In this model there are five distinct security zones, ranging from the lowest-security level or zone zero, which comprises publicly accessible spaces, to the highest-security level or zone four, where confidential data is processed or stored. The deployment of video surveillance cameras in these zones is based on risk assessments by the EPO which are detailed in the record of processing activities for the VSS.

Areas subject to heightened expectations of privacy, such as offices, leisure areas, canteens, bars, cafeterias, toilets, showers and changing rooms, are not monitored.

A data protection impact analysis is conducted in all cases where the processing operation is likely to result in a high risk to the rights and freedoms of data subjects.

Information on the existence of the VSS is be made available to the staff and public. This information is provided in a layered approach by means of signs and the publication of a Video Surveillance Policy (Circular 421).

Purpose of Processing The purpose of the processing operations is to be able to address the security and operational safety concerns efficiently, validate identities, how people are able to access its buildings and how people are able to access its information processing facilities (e.g. EPO Data Centre). In a regular basis the system is used to verify the perimeter of our buildings, access to these ones and to areas where sensitive information is processed and thus enhance the protection of intellectual property and sensitive information processed and stored in our premises. In case of incidents such as intrusions, theft or evacuation, the system is also used to support the operational safety activities of the external security contractor responsible for the execution of those processes.

Data Retention Considering the lawful basis and purposes established for processing personal data using the VSS, the maximum retention period established for images captured is set to a 7 days period, time after which the images are automatically erased.

This retention period can be extended for backups of images related to identified incidents where the footage becomes part of the evidence to support investigations, appeals, litigation or claims. It can be extended until the investigations, appeals, litigation or claims are resolved.

This retention period can be extended for backups of images related to identified incidents, where the footage becomes part of the evidence to support investigations, appeals, litigations or claims until those ones are resolved.

Data subjects and categories of personal data

Contractors

Matter/Log file	
Metadata	
Sensory and Electronic Information	
Thermal Information	Time stamps from their access to the buildings
Visual Information	
Physical and/or Digital Identifiable Assets	
Digital Certificate	
Device Management Data	
Account ID	Encryption Keys
Last Logon Time	MAC Address
Personal Identification	
Full Name	
User Account Information	
User ID	
Government Identifiers	
Driving Licence Number	
System Logs	
Audit Logs (a.k.a. Audit Trail)	File data (name, size and/or hash)
Firewall/Router/Switch Logs	Ports
Registry data	Running Processes

System-, Application-, Security-related Server Logs	Transaction-related Details
Web Servers Logs	

Employees

Matter/Log file	
Metadata	
Sensory and Electronic Information	
Thermal Information	Time stamps from their access to the buildings
Visual Information	
Physical and/or Digital Identifiable Assets	
Digital Certificate	
Device Management Data	
Account ID	Encryption Keys
Last Logon Time	MAC Address
Windows ID for Windows Devices	
User Account Information	
User ID	
Government Identifiers	
Car registration documents	
System Logs	
Audit Logs (a.k.a. Audit Trail)	File data (name, size and/or hash)
Firewall/Router/Switch Logs	Ports
Registry data	Running Processes
System-, Application-, Security-related Server Logs	Transaction-related Details
Web Servers Logs	

Externals

Sensory and Electronic Information	
Visual Information	

Recipient of the personal data

Recipients of the data Personal data processed or stored in the VSS is used only internally by the EPO department operating the VSS and staff of its external security contractor to assist them in the performance of their duties (monitoring and managing security and safety processes, responding to alarms).

The EPO Building Maintenance Team's experts technicians, the external maintenance company technicians and the external safety experts have access to the application and its hardware for the performance of the maintenance of those ones.

The Operations Office Security staff and the external security provider can access one hour back the recordings for alarm processing, this way incidents in areas where the event happened in the last 60 minutes can be verified and discarded or processed more efficiently.

In the event of highly unsafe driving behaviour, the delegated controller can provide access to the video footage of the incident to the EPO safety experts for their analysis and expert advice.

In the case of accidents or incidents that entail insurance claims, the delegated controller can also provide access to the relevant video footage to the company processing the claim, provided all the relevant provisions of the EPO data protection rules (DPR) for such disclosure are respected.

All other cases are covered under OW-SOP-2022-004-F

Purpose of sharing See para. 1.23

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation
Transfers of personal data collected by the VSS to recipients outside the EPO can take place when relevant under the duty to co-operate with the competent authorities of
the contracting states pursuant Article 20 of the Protocol on Privileges and Immunities of the European Patent Organisation.

A registry to document such transmissions, including their legal basis, date, time, type of personal data transmitted and recipients is accurately maintained by the delegated controller.

Transfer mechanism(s) Legally binding and enforceable instrument between public authorities or bodies, Derogation in accordance with Art. 10 DPR

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer Public Authorities/Government Bodies

Derogations Art. 10 DPR The transfer is necessary for the performance of a task in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning, or to perform obligations arising from its duty of co-operation with the contracting states, The data transfer is necessary for the establishment, exercise or defence of legal claims and their transmission is not precluded by agreements under international law or other applicable legal provisions of the European Patent Organisation

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network	

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 148

Name Workflows in the Patent Workbench

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 46 - CIO / BIT

Entity Name - Controller (Entities) DG1 - 1 - Patent Granting Process, DG1 - 11 - COO

Description of the processing

Description The following generic task workflow covers the Search, Examination and Opposition workflows, as well as actions specific to Formality Officers and to the Quality Auditors. Specificities of each workflow is detailed in the next section.

GENERIC TASK WORKFLOW:

1. An event (Muse, online filing, answer from the applicant, PWB action, …) automatically triggers an action task creation in the PWB and provides data to the PWB.

2. PWB then automatically assigns the action task to an Examiner or a Formality Officers whose duty is to perform an action.

3. The action is manually performed by the Examiner or Formality Officer either in tools outside the PWB or directly within the PWB. The outcome of the action is the generation of a document, or a set of documents stored outside the PWB. Completion of the action is automatically logged in the PWB and triggers step 4. for examiners' actions and step 7. for Formality Officers' actions.

4. The PWB automatically circulates a review task to Review Members in charge of the review task who have the duty to review the action performed in step 3. Each of them has to log manually whether the action is approved or not in the review task and can optionally enter comments that are visible for all members involved in step 3 to 6b.

5. If any of the members in charge of the review task of Step 4. logs manually a non-approval of the action, this triggers the process to returns automatically to step 2. This loop is repeated as many times as necessary as long as a non-approval is logged manually by any members in charge of the review task of step 4.

6. If all members in charge of the review task log manually the approval of the action, then the action task and review tasks are automatically closed and archived, and either

6a. the formality Officers performs manually a further processing of the action and action documents with a tool outside PWB; or

6b. for enhanced flows, PWB directly generates the documents, sends them to the applicant and updates the legacy tools.

7. The action task performed by Formality Officers in step 3 is closed and archived, …
7a. automatically when the Formality Officer terminates the actions in PWB; or
7b. manually by an employee of the Finance department, after the Formality Officer has manually transmitted (=Trigger) the action to the finance department through PWB.

PROCESSING PERSONS IN SPECIFIC WORKFLOWS

The Review Members of steps 4-6 for tasks performed by Examiners in step 3. are:
- For Search actions: the Line Managers and their deputies, Formalities Officers and eventually the Chairperson in case of positive search

- For summons to oral proceedings in examination: The Examining division, the Line Managers and their deputies, Formalities Officers.

- For minutes of Oral proceedings: the Chairperson, the Line Managers and their deputies, Formalities Officers.

- For examination IGRA (Intention to GRAnt) and Refusals: The Examining division, the Line Manager and their deputies, Formalities Officers, and eventually Quality Auditors* for IGRAs.

- For enhanced flows (eComm, ePrep, eTel, eOR9C): The Examining division, the Line Manger and his deputies (and optionally Formality Officer if the automatic process).

- For other examination Tasks: The Line Manger and his deputies, Formality Officers.

- For tasks of the opposition division: The opposition division, the Line Manager and his deputies, Formality Officers.

- For all actions, there is the possibility to add a Legal Member (DG5) in the review process.

* Quality Audit: for IGRA review, after the Line manager has approved the IGRA task, and before the Formality Officers perform their review, actions are randomly sampled and fill a buffer from which Quality Auditors can select a task. The Quality Auditor has access to all data in PWB and can interact with the division exclusively. Discussion between the quality auditor and the division happens outside PWB and no information is shared with the line manager. Only Formalities Officers can retrieve the information that the file has been sampled for the DQA checks.

No review process is in place for actions performed by Formality Officer in steps 3 and 6-7a.

Purpose of Processing The purpose of this processing is to ensure a seamless workflow and communication between the EPO employees involved in the patent granting process. Processing contact data is needed to perform the routing of tasks between employees involved in the patent granting process and enable communication between them. Processing Log data and comments is needed to enable communication completeness and timeliness of the task execution. Moreover, user might need to retrieve previous comments when checking again the same task. (Legal Basis: see document “New data protection rules – alignment with the patent grant procedure”)

Software and Databases involved in the Workflow

- Steps 1, 3 and 7: Triggers and data from the external events or previous step events are collected in Kafka with a retention time of 7 days.
- Steps 1-7b: All data about the task and its processing steps (including userID, logs and comments) is processed by the Camunda Process Engine and stored in the Mongo Database. There is one specific Process Engine and one specific Mongo Database for each of these processes: Search, Examination and Opposition. Retention time: unlimited.
- Steps 1-7b: status and history of the task is visible in the PWB for all involved employees (examiners, LM, FO) for 30 days after completion of the task. Retention of these history data is in “Elastic Store” and limited to 30 days after completion of the task.

Data Retention Retention Period:

For Kafka: 7 days
For the Process Engines and Mongo DB: unlimited (legal basis: see document “New data protection rules – alignment with the patent grant procedure”)
For the Elastic Store : 30 days

Data subjects and categories of personal data

Employees

Network/application Interaction Data	
Session details	
Contact Information	
Contact Details	
Correspondence	
Personal information provided voluntarily	
Employment Information	
Business Unit Division	Job Title Role
Line Reporting Manager	
Personal Identification	
Full Name	
User Account Information	
User ID	

Externals

Network/application Interaction Data	
Session details	

Contact Information	
Contact Details	
European Patent Register Data	
Data provided by the data subjects	
Correspondence	
Personal information provided voluntarily	
Personal Identification	
Full Name	

Recipient of the personal data

Recipients of the data EPO employees involved in the processing steps 1 to 7 will have access to the data during the task processing, and in their history function for 30 days after the task has been terminated.
Line managers + deputies will have access to the data during the task processing, and in their history function for 30 days after they terminate the task.
IT administrators have access to all data for maintenance and support.
EPO Service Line internal employees have access to the PWB tool for technical support.
A daily snapshot of the Camunda Process Engines for Search and Examination is copied by department 4612 (Business Analytics CoE) in the Data Warehouse, comprising all data except the comments/notes of the users. No manual nor automatic analysis processing of the captured data is performed by department 4612. These data can be accessed for analysis purpose by users in Dir. 141 (Business Analysis and Planning) and department 1341 (Quality and Risk Analysis).

Purpose of sharing Personal Data are processed for following persons:
DG1 examiners, DG5 Legal member, DG1 Formalities Officers, line manager
Data from the applicant and/or its legal representative.
All processed data are business related and contain no sensitive personal data.
Moreover, data relating to the applicant, the legal representatives and the identity of the examining division members are public data for the patent grant process.
Processed data:
Name of the applicant
Links to the action document(s) which includes eventually contact data about the applicant, employees of the applicant, legal representative of the applicant, or professional contact data of the EPO employee.
First and last name, userID, Team, Directorate and role of the EPO employees involved in the processing steps 1 to 5d, as well as the name of their line managers and directors.
Logging date/time, Approval/non-approval logs, and comments of EPO employees involved in the processing steps 1 to 5d.

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 150

Name Amicable Settlement Attempt

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 42 - People, DG0 - 045 - Internal Audit and Professional Standards - Ombuds Office, DG0 - 06 - Appeal Committee Secretariat, DG4 - 43 - Welfare & Remuneration, DG4 - 4 - Corporate Services, DG4 - 41 - Finance

Entity Name - Controller (Entities) DG0 - 08 - Employment Law and Social Dialogue Advice

External processors

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

OpenText

External processors	
Name OpenText	

Microsoft

External processors	
Name Microsoft	

OpenText

External processors

Name
OpenText

TRE Thomson Reuters

External processors
Name
TRE Thomson Reuters

Microsoft

External processors
Name
Microsoft

Description of the processing

Description The data controller's involvement in the amicable settlement procedure and the corresponding collection and processing of personal data is triggered at the pre-litigation and/or litigation stages as defined in Article 106-113 Service Regulations for permanent and other employees.

Principal Directorate Employment Law and Social Dialogue Advice (PD08) Lawyers identify cases that may be appropriate for settlement. Efforts to reach an amicable settlement focus mainly on cases before they are placed on the agenda of the Internal Appeals Committee ('ApC') or the Administrative Tribunal of the International Labour Organization ('ILOAT').

The ApC can also enquire (by e-mail) about the possibility of an amicable settlement in the cases placed on their agenda. Prior to the commencement of an ILOAT session, a similar procedure conducted by the ILOAT Registrar applies.

PD08 Lawyers process the personal data contained in the communications and submissions put forward by the data subject and the Office during pre-litigation or litigation to determine whether the case is appropriate for settlement and if so, on what basis/terms.

The data processed for the amicable settlement is taken from the case file stored on the document management systems (Mattersphere and OpenText). PD08 lawyers check the facts of the case for accuracy. Additional data is collected when it is necessary to update the file.

Depending on the subject matter of the proceedings, it might require the processing of special categories of data and/or third parties' data. In such a case, personal data are processed on the basis of Article 11(2)(b), (e), (f) and Article 11(3) DPR.

Depending on the subject matter of the proceedings, it might require the processing of personal data relating to criminal convictions and offences. In such a case, personal data are processed on the basis of Article 12(1) DPR: The processing is covered by legal provisions of the European Patent Organisation providing for appropriate safeguards for the rights and freedoms of data subjects.

Processing under Article 11 and 12 takes place under the condition that the processing is necessary to the adjudication of the case and proportional to the purpose (the assessment of necessity and

proportionality is carried out on a case-by-case basis). Depending on the case, these data are requested in a manner that renders it anonymised or, at least, pseudonymised in a way that will not allow PD08 or delegated controller(s) further processing the data to re-identify the data subjects unless after applying these techniques, the data can no longer be meaningfully used for the performance of PD08's activities. In this case, only the minimum information strictly necessary should be processed on a case-by-case basis and in compliance with the principle of confidentiality. Techniques for anonymisation or pseudonymisation are also used when submitting such data to another delegated controller(s), if required.

A proposal for a settlement attempt including a statement of reasons is prepared by the PD08 Lawyers and sent to the hierarchy for approval by e-mail, or in a note to the President (NttP) via the Common Log System (OpenText).

The competent authority responsible for deciding on the amicable settlement depends on the amount of the proposed envelope.

In the event a settlement proposal is approved by hierarchy, the settlement proposal is prepared by PD08 Lawyers and sent to the data subject involved by the Employment Law Secretariat via email including an invitation to the data subject, or their (legal) representative / successor, if applicable to enter settlement negotiations.

The Employment Law Secretariat may send and receive further email correspondences to/from the data subject or their (legal) representative / successor.

Settlement negotiations may take place between the PD08 staff, the operational unit involved, the Human Resources Business Partner ('HRBP') and the data subject and their (legal) representative / successor in writing, in person or via (video) call (Microsoft Teams, Zoom).

Depending on the case, other business units may be involved in the fulfilment of certain supplementary tasks, such as facilitation of settlement negotiations and execution of the settlement.

Depending on the subject matter of the case, the types of personal data processed may differ.

The entire settlement procedure is strictly confidential.

The conclusion of the settlement negotiations, including the settlement agreement if applicable, shall be set out in writing to the data subject drafted by the PD08 Lawyer and sent to the data subject in an email or as an attachment in an e-mail. The email is sent by the Employment Law Secretariat.

If the person concerned accepts or rejects a settlement attempt, the settlement procedure ends.

Depending on the case, the ApC Secretariat or the ILOAT Registrar will be informed about the outcome of the settlement procedure.

Informal exchanges are conducted via email. Draft documents and other files are exchanged via email or are accessible internally through a link to OpenText sent in an email.

Data processing is done electronically as the data including the case file with all correspondence between the data subject and the Office inviting them to settlement negotiations are all stored on electronic PDF, word or excel files and stored on MatterSphere or on the OpenText. In the event a settlement attempt must be approved by the President, the NttPs are stored also on the CommonLog.

Purpose of Processing Providing an archive of legal reference for PD08 Lawyers using the tool 'Caseload' (Excel), MatterSphere and OpenText., Depending on the case, sharing information uncovered with internal business units (inter alia HRBP, HR, Finance, Line Manager) that is in their interest to be aware of and may also help to promote social dialogue on a case-by-case basis, insofar as this is compatible with the principle of confidentiality., Prepare legal analysis for hierarchy to identify trends and assess effectiveness of legal arguments over time., The monitoring of deadlines via the tool 'Caseload'., Providing PD08 Lawyers with an understanding of the legal issue and the surrounding circumstances., Providing the data subject with sufficient and coherent reasoning in the conclusion of the settlement procedure., Preparing statistics, lists and analysis for the hierarchy, if requested., The promotion of social dialogue., Establishing all of the facts and providing comprehensive legal input to the competent authority taking the decision on the settlement proposal., The amicable settlement of disputes as requested in Communiqué 30.10.2018 and provided for in Article 6 of the Impl. Rules to Article 106-113 ServRegs.

The procedural steps, including settlement initiatives and the outcome of amicable settlement attempts is recorded on the tool ‘Caseload’ (excel) by the Employment Law Secretariat.

Employment Law Secretariat maintains a database of cases appropriate for settlement and the status/success of amicable settlement negotiations. This settlement list is stored on Microsoft excel.

Paper files are scanned into the system and are then stored in the physical case file. The creation of physical files has ceased since mid-2018.

To avoid conflict of interest, the procedure may differ for instance if a PD08 staff member is a party of the settlement procedure.

The processing of personal data is necessary in order to address all aspects related to the consequences of the settlement, the creation of statistics and lists and the legal analysis, if necessary.

Data Retention Personal data concerning the settlement procedure will be stored until the last day of the 10th calendar year after closure of the settlement procedure.

The data retention period for specific categories of personal data (e.g., name of employee, case number, outcome, key milestones) stored in “MatterSphere” and “Caseload”, relevant for workflow tracking, archiving, research or statistical purposes, ends on the last day of the 50th calendar year following the expiration of the respective periods mentioned above.

After expiry of the 50-years’ period, the data categories shall be anonymised and kept indefinitely for archiving purposes in the legitimate exercise of the official activities of the European Patent Organisation, as provided for in Article 20(3)(d) DPR.

Files uploaded to the Common Log system (OpenText) are stored commensurate with the retention period defined by the data controller of the Common Log system.

The retention time applies to both, electronic and paper files.

Data subjects and categories of personal data

Employees

Applications' Log	
SAP Logs	
Social	
Social Media Account	Social Media Contact
Social Media History	
Sensory and Electronic Information	
Audio Information	Electronic Information
Presence Status	Thermal Information

Time stamps from their access to the buildings	Visual Information
Building area and site	
Building area and site	
Representation in EPO's Patent Granting Process	
Affiliation to Association of professional representatives	All data provided upon request for entry or change
Authorisee function	Authorisor function
EPO CDS (Client Data System) categories related to the Representation role	Representative registration number (ID)
Role in the Patent Grant Procedure	Supporting documentation
Telephony Interaction Data	
Recorded Audio File	Telephony Session Content
Telephony Session Details	Telephony Session Metadata
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name
Gender	Height
Surname	Marital Status
Nationality	Picture
Racial or Ethnic Origin	Religion/Religious Beliefs
Sexual Orientation	Signature
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
Project management experience	

Matter/Log file	
Attachments	Metadata
General	
Answers to surveys, assessments or quizzes	Any other information
Assessment and legal opinions	Input provided during the deliberation and decision-making process
Legal opinions and assessments	Nomination justificative
Personal Information in SAP	Sensitive Personal Data in SAP
Special Categories of Data in SAP	User association
Workplace Welfare	
Records of Personal Properties	
Contact Information	
Contact Details	Country
Emergency Contact Details	Home Address
Home Leave Address	Mobile Phone Number
Personal Email	Phone Numbers
Previous Residence Address	Private Phone Number
Teleworking address	Working email address
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
Diagnostic tools' results	IDP
Instructor related data	Learning external events
Learning history	Learning plan
Ratings	Social learning inputs
Device Management Data	
Account ID	AppleID for iOS/iPadOS Devices
Azure Active Directory Device ID	EAS Device ID
Encryption Keys	Intune Device ID

Intune Device Management ID	Last Logon Time
MAC Address	Managed Application Device Tag
Managed Application ID	Platform-specific IDs
Tenant ID	Windows ID for Windows Devices
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of a patent (claims, description, drawings, abstract)
Personal data potentially included within the content of patent procedure related information and publications	
Health Insurance Information	
Insurance Policy Information	Unique Identifier for Subscriber
System Logs	
Audit Logs (a.k.a. Audit Trail)	File data (name, size and/or hash)
Firewall/Router/Switch Logs	Ports
Registry data	Running Processes
System-, Application-, Security-related Server Logs	Transaction-related Details
Web Servers Logs	
Phone Call Information	
Called Phone Number	Caller's Phone Number
Phone Call Date and/or Time	Phone Call Duration
Phone Call Interaction History	Phone Calling History
Ticketing	
Ticket related data	
Physical and/or Digital Identifiable Assets	
Digital Certificate	ICCID (Integrated Circuit Card Identification Number)

IMEI Number (International Mobile Equipment Identity)	Mobile Device Name
Mobile Device Serial Number	Mobile Device's Network Adapter MAC Adress
Operating System Version	Pod Internal Id
Smart Card Number	Videoconference Room/Equipment Identifier
Workstation Serial Number	Workstation's Hostname (Physical or Virtual)
Workstation's Network Adapter MAC address	
Biometric	
Body temperature	Facial Recognition
Fingerprint	Voice Recognition
Online invigilation data	
Audio input	Webcam captures
Background Checks	
Criminal History	Criminal Records
Drug Test Results	Reference or Background Checks
Employment Information	
Active/Inactive Indicator	Appeals Records Information
Assessment and legal opinions	Benefits and Entitlements Data
Business Unit Division	Company Entity
Contract Type	Corporate Credit or Debit Card Numbers
Department name and/or number	Disciplinary Action
Duration of employment	End Date
End Date and Reason for Termination	EPO access badge number
Exit Interview and Comments	Grade
Grievances and Complaints	Hours of Work
Job Application Details	Job Group
Job Title Role	Language preference (of communication)
Line Reporting Manager	Membership in a EPO Staff Committee

Military Status	Office Location
Performance Rating	Personnel Number
Previous Work History	Record of Absence/Time Tracking/Annual Leave
Record of Maternity Leave	Rewards history
Room Number	Salary
Start Date	Weight
Unknown	
EPO badge validity	Identification of which membership is envisaged
Price list for discounts	
Geolocation	
Geolocation Information	
Network/application Interaction Data	
Results on phishing attempts (entered credential not processed)	Session content
Session details	Session metadata
Health Data	
Dietary requirements	Health Data
Mobility needs	
Professional Experience & Affiliations	
Affiliation	CV
Entry or deletion date as member of an association	Political Affiliation and Activities
Professional Memberships	Qualifications Certifications
Trade Union Membership	
Examination content data	
Examination marks	Examination result
Family Information	
Child’s Level/Year of Studies	Child’s School Enrolment Date Start
Children's Names	Child's birthday

Composition of the family (number of dependent children/persons)	Parents' Names
Spouse's information	Spouse's name
Financial	
Bank Account Information	Bank Account Number
Bank details	Bank Statements
Bonus Payments	Compensation Data
Credit Card Number	Credit History
Debit Card Number	Deposit Account
Fund Reservation Requests	Information on home loans
Insurance Information	Routing Number
Browsing Information	
Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
Category	Cookie Information
IP Address	Network Interaction History
URL	Website History
User Account Information	
Account Age	Account Number
Account Password	Application Specific User Role
Membership Permissions	Ownership Permissions
Password	Password Hash
Third-party User Identifier	User ID
Government Identifiers	
Car registration documents	Driving Licence Number
ID/Passport picture	National Identification Number
National Identity Card Details	Passport Number

Social Security Number	

Former Employees

Applications' Log	
SAP Logs	
Social	
Social Media Account	Social Media Contact
Social Media History	
Sensory and Electronic Information	
Audio Information	Electronic Information
Presence Status	Thermal Information
Time stamps from their access to the buildings	Visual Information
Building area and site	
Building area and site	
Representation in EPO's Patent Granting Process	
Affiliation to Association of professional representatives	All data provided upon request for entry or change
Authorisee function	Authorisor function
EPO CDS (Client Data System) categories related to the Representation role	Representative registration number (ID)
Role in the Patent Grant Procedure	Supporting documentation
Telephony Interaction Data	
Recorded Audio File	Telephony Session Content
Telephony Session Details	Telephony Session Metadata
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition

First Name	Full Name
Gender	Height
Surname	Marital Status
Nationality	Picture
Racial or Ethnic Origin	Religion/Religious Beliefs
Sexual Orientation	Signature
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
Project management experience	
Matter/Log file	
Attachments	Metadata
General	
Answers to surveys, assessments or quizzes	Any other information
Input provided during the deliberation and decision-making process	Legal opinions and assessments
Nomination justificative	Personal Information in SAP
Sensitive Personal Data in SAP	Special Categories of Data in SAP
User association	
Workplace Welfare	
Records of Personal Properties	
Contact Information	
Contact Details	Country
Emergency Contact Details	Home Address
Home Leave Address	Mobile Phone Number
Personal Email	Phone Numbers
Previous Residence Address	Private Phone Number
Teleworking address	Working email address

Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
IDP	Instructor related data
Learning external events	Learning history
Learning plan	Social learning inputs
Device Management Data	
Account ID	AppleID for iOS/iPadOS Devices
Azure Active Directory Device ID	EAS Device ID
Encryption Keys	Intune Device ID
Intune Device Management ID	Last Logon Time
MAC Address	Managed Application Device Tag
Managed Application ID	Platform-specific IDs
Tenant ID	Windows ID for Windows Devices
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of a patent (claims, description, drawings, abstract)
Personal data potentially included within the content of patent procedure related information and publications	
Health Insurance Information	
Insurance Policy Information	Unique Identifier for Subscriber
System Logs	
Audit Logs (a.k.a. Audit Trail)	File data (name, size and/or hash)
Firewall/Router/Switch Logs	Ports
Registry data	Running Processes
System-, Application-, Security-related Server Logs	Transaction-related Details

Web Servers Logs	
Phone Call Information	
Called Phone Number	Caller's Phone Number
Phone Call Date and/or Time	Phone Call Duration
Phone Call Interaction History	Phone Calling History
Ticketing	
Ticket related data	
Physical and/or Digital Identifiable Assets	
Digital Certificate	ICCID (Integrated Circuit Card Identification Number)
IMEI Number (International Mobile Equipment Identity)	Mobile Device Name
Mobile Device Serial Number	Mobile Device's Network Adapter MAC Adress
Operating System Version	Pod Internal Id
Smart Card Number	Videoconference Room/Equipment Identifier
Workstation Serial Number	Workstation's Hostname (Physical or Virtual)
Workstation's Network Adapter MAC address	
Biometric	
Body temperature	Facial Recognition
Fingerprint	Voice Recognition
Online invigilation data	
Audio input	Webcam captures
Background Checks	
Criminal History	Criminal Records
Drug Test Results	Reference or Background Checks
Employment Information	
Active/Inactive Indicator	Appeals Records Information
Benefits and Entitlements Data	Business Unit Division
Company Entity	Contract Type

Corporate Credit or Debit Card Numbers	Department name and/or number
Disciplinary Action	Duration of employment
End Date	End Date and Reason for Termination
EPO access badge number	Exit Interview and Comments
Grade	Grievances and Complaints
Hours of Work	Job Application Details
Job Group	Job Title Role
Language preference (of communication)	Line Reporting Manager
Membership in a EPO Staff Committee	Military Status
Office Location	Performance Rating
Personnel Number	Previous Work History
Record of Absence/Time Tracking/Annual Leave	Record of Maternity Leave
Rewards history	Room Number
Salary	Start Date
Weight	
Unknown	
EPO badge validity	Identification of which membership is envisaged
Price list for discounts	
Geolocation	
Geolocation Information	
Network/application Interaction Data	
Results on phishing attempts (entered credential not processed)	Session content
Session details	Session metadata
Health Data	
Dietary requirements	Health Data
Mobility needs	
Professional Experience & Affiliations	

Affiliation	CV
Entry or deletion date as member of an association	Political Affiliation and Activities
Professional Memberships	Qualifications Certifications
Trade Union Membership	
Examination content data	
Examination marks	Examination result
Family Information	
Children's Names	Parents' Names
Spouse's information	Spouse's name
Financial	
Bank Account Information	Bank Account Number
Bank details	Bank Statements
Bonus Payments	Compensation Data
Credit Card Number	Credit History
Debit Card Number	Deposit Account
Fund Reservation Requests	Information on home loans
Insurance Information	Routing Number
Browsing Information	
Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
Category	Cookie Information
IP Address	Network Interaction History
URL	Website History
User Account Information	
Account Age	Account Number
Account Password	Application Specific User Role
Membership Permissions	Ownership Permissions

Password	Password Hash
Third-party User Identifier	User ID
Government Identifiers	
Driving Licence Number	ID/Passport picture
National Identification Number	National Identity Card Details
Passport Number	Social Security Number

Externals

General	
Legal opinions and assessments	
Contact Information	
Working email address	
Employment Information	
Job Title Role	
Personal Identification	
Full Name	

Recipient of the personal data

Recipients of the data Recipients within the EPO:
• Members of the Internal Appeals Committee
• Appeals Committee Secretariat
• Internal business units (e.g., the Ombuds Office, HRBPs, Finance, HR services, Welfare & Remuneration, Line Manager) whose involvement is necessary and required in the fulfilment of certain supplementary tasks such as the facilitation of settlement negotiations, the execution of the settlement and the preparation of statistics, lists and analysis, on a case-by-case basis, insofar as this is compatible with the principle of confidentiality

Recipients outside the EPO:
• The Tribunal (ILOAT).
• The external law firms representing the EPO before the ILOAT.
• The data subject's (legal) representative / successors where they are engaged in settlement negotiations.

Purpose of sharing

Transfer

Transfer Yes

Country where data might be transferred - Processor (Vendors) TRE Thomson Reuters - Luxembourg, OpenText - United Kingdom, Microsoft - United States

Transfer to public authority and/or International Organisation International Labour Organisation Administrative Tribunal - Switzerland

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, If the data controller's involvement in the amicable settlement procedure and the corresponding collection and processing of personal data is triggered at the litigation stages before ILOAT (e.g., upon the request of ILOAT), specific categories of personal data is provided to the ILOAT.

Transfer mechanism(s) The recipient provided appropriate safeguards, Data Protection EU Comm Standard Contractual Clauses

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 159

Name Access Control and Card Management Systems - DG4 -PD44 - General Administration

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 44 - General Administration

Entity Name - Controller (Entities) DG4 - 44 - General Administration

External processors

Security Services Contractor at the EPO site of Munich

External processors	
Name Security Services Contractor at the EPO site of Munich	

Security Services Contractor at the EPO site of Berlin

External processors	
Name Security Services Contractor at the EPO site of Berlin	

Security Services Contractor at the EPO site of The Hague

External processors	
Name Security Services Contractor at the EPO site of The Hague	

Security Services Contractor at the EPO site of Vienna

External processors

Name

Security Services Contractor at the EPO site of Vienna

Description of the processing

Description The Card Management System is used to register the data subjects and to provide them with access badges to be used to enter the EPO premises in a controlled way.
Prior to production of the access cards, the identity of the recipients and the authenticity of the document presented is verified by means of identity document scanners.
During the process the data in the document and the chip (if available) is verified and immediately discarded once the result is presented. There is no data recorded.
The access control system (AEOS) is a software application that is used Office-wide to manage access within the different EPO sites and is managed by the Facility Management Directorate.
The AEOS application registers EPO staff, contractors, service providers and visitors via web server application installed under EPO servers.
The application is connected to the card management system (CMS Nexus Prime application which is fed by SAP FIPS), from which it receives the information. In addition to the data fields exported by the CMS, AEOS stores also the access profiles of each data subject and the access logs of the readers where the users presented their access badge, regardless to whether access is granted or not.
All data received by the access control system comes from FIPS via the card management system.
The access profiles are used to grant or deny access to individual access points (card readers) in the EPO buildings.

VISITOR ACCESS
The system is also used for registering and granting access to visitors in the sites where access control readers are installed. In those sites the external security provider registers visitors at the reception of each building using the AEOS application. The data is then stored in a central access control database and used to distribute the right badge that each visitor is requested to wear during the time of their visit. The data registered from visitors is obtained from their identity document and includes some of the details mentioned in the identity document presented by the visitor including name, family name, date of birth and/or identity document number. In addition there are some other details including visitor badge number, contact person and company also added to AEOS.
For EPO's employees family members (FIPS registered partners and dependent children from EPO staff above the age of 16), personal data are processed in order to provide them a family badge to access the EPO sport facilities and semi-public areas if so requested via MyFIPS interface by the sponsoring staff member. The badge will contain their picture, full name and ref. to the EPO staff member that is linked to the family member.
Additionally the EPO Fitness Club Manager will use it to register fitness club members and give them access to the fitness rooms. There is an automated e-mail sent to individual fitness club members when their membership to the club is due to expire.
All data categories contained in a travel document (passport or national identity card) are processed but not stored. They are only processed during the identity verification done by means of identity document scanners being discarded once the result is presented.

REMOTE PROVISION OF BADGES TO PATENT ATTORNEY
Patent attorneys can request a badge remotely. The production of EPO badges for professional representatives is done by pre-arranged video call. During the call the professional representative will need to show their passport or national ID card. The badge will then be produced and sent by mail to them. The EPO badge enables professional representatives to identify themselves in oral proceedings

Purpose of Processing The card management system application is used to: 1. Manage access badges to provide access to buildings to EPO staff, family members, Council members, patent attorneys, contractors, EPO pensioners, service providers and visitors; 2. Verify that the visitors are not in the House Ban list (See Genehmigungsschreiben of 288/16) and as such allowed to enter the EPO Premises before a visitor badge is assigned to them; Verify the identity of the persons getting an EPO access badge by means of automated identity scanners, which at the same time also verify the authenticity of the identity document scanned. In the access control system personal data is processed for the purpose of managing access to the different EPO buildings and parking facilities in an efficient and effective way. The access control system is also used to monitor compliance with the existing provisions (House Rules and Security Circulars) as well as to: 1.- Provide access to EPO staff, visitors and contractors, including service providers, to EPO buildings; 2.- Register the access logs to areas where access has been granted to users; 3.- Register in an automated way (upon arrival of the vehicle to the entrance of the parking) the vehicle number plate of staff, contractors and visitors vehicles having access to EPO premises in order to: a) Monitor parking usage and limit the intervention of administrative staff for the registration of long term parking requests. b) Automate the way staff is informed whenever they violate the parking rules leaving their vehicles for longer terms than permitted (e.g. sending automated e-mails to staff not respecting the parking

and consultations (by video conference or on site) and to access EPO premises, e.g. rooms for oral proceedings, as well as the canteens and coffee bars.

CO2 EMISSIONS
In order to calculate the impact that the usage of private own staff vehicles have on CO2 emissions, the access control database from the AEOS application, is queried by an algorithm (via SQL script), programmed by the company NSecure, that extracts the amount of vehicles belonging to permanent employees that access the parking facilities in Munich and The Hague.
In Munich, this is done by analysing the number of permanent employees presenting their badge in the access control readers that provide access to the parking lots in their premises.
In The Hague site this is done by querying the same data group but extracted from the Automatic Number Plate Recognition system (ANPR) cameras that are located at the entrance of the parking lot of that site.
The results of both data sets are an anonymous statistical data set that contains only figures related to each site, serving as base for the analysis of the CO2 impact that The Office envisages to collect and analyse. The information is provided via e-mail Excel attachment sent by the access control software AEOS using the SMTP email server of the EPO as runway.

OCCUPANCY RATE MONITORING
To monitor the usage and occupancy rates of the buildings the room and department number are added to the card management and access control system. The verification is done anonymously to indicate the percentage of buildings' usage, floors and departments without analysing individual usage but organisational unit occupancy of allocated and non-allocated rooms.

Groups or persons concerned:
- EPO employees
- EPO employees family members (above the age of sixteen)
- EPO pensioners
- Visitors
- Service providers
- Canteen users
- External persons
- DPMA Berlin Office staff
- Patent Attorneys
- Council members.

Link to Notice OJ: https://www.epo.org/en/legal/official-journal/2021/10/a79.html

rules). c) Manage in a more efficient way the available parking facilities (one vehicle per staff member). To achieve No. 3, the number plates of the vehicles approaching the entrance of the parking are registered and linked to their access badge, this is done in order to identify the owner of the vehicle and to be able to monitor parking usage (one vehicle per person, one day maximum allowed parking time). 4.- Trigger alarms via Security Management System including door too long open alarms, forced opening of an entrance door or perimeter door and non-authorised badge used in an entrance.

Data Retention ACCESS CONTROL SYSTEM
Access logs older than 12 months will be overwritten by an automated routine programmed in the software.
Visitor data will only be kept for 28 days in line with the video surveillance records and for security purposes. This will allow physical security to proceed supporting investigations involving visitors access if criminal offences are reported.
In the event of a formal appeal/litigation, all data held at the time of the formal appeal/litigation shall be retained until the completion of its process.

CARD MANAGEMENT SYSTEM
Data coming from FIPS will be stored and deleted following the retention times established by FIPS (an employee or contractor user data will be deleted upon deletion in FIPS).
For groups such as the Administrative Council or Patent Attorneys added manually by the so-called data manager, this one will perform, at least once per year or whenever a change is reported to them, a sanity check. During this check the data manager will verify if the data is still valid and correct, performing any necessary changes and/or deletions to keep the data up to date.
In the event of a formal appeal/litigation, all data held at the time of the formal appeal/litigation shall be retained until the completion of its process.

Data subjects and categories of personal data

Employees

Sensory and Electronic Information	
Time stamps from their access to the buildings	
Contact Information	
Phone Numbers	Working email address
Employment Information	
Benefits and Entitlements Data	Business Unit Division
End Date	EPO access badge number
Language preference (of communication)	Office Location
Room Number	Start Date
Personal Identification	
Full Name	Gender
Unknown	
EPO badge validity	Price list for discounts
Government Identifiers	
Passport Number	

Contractors

Sensory and Electronic Information	
Time stamps from their access to the buildings	
Contact Information	
Phone Numbers	Working email address
Employment Information	
Business Unit Division	End Date
EPO access badge number	Language preference (of communication)
Office Location	Room Number
Start Date	
Personal Identification	
Full Name	Gender
Unknown	
EPO badge validity	Price list for discounts
Government Identifiers	
Passport Number	

Externals

Sensory and Electronic Information	
Time stamps from their access to the buildings	
Employment Information	
EPO access badge number	
Unknown	
EPO badge validity	
Personal Identification	
Date of Birth	Full Name
Government Identifiers	
National Identity Card Details	Passport Number

Former Employees

Sensory and Electronic Information

Time stamps from their access to the buildings	
Contact Information	
Personal Email	
Employment Information	
End Date	EPO access badge number
Personnel Number	
Personal Identification	
Full Name	
Unknown	
EPO badge validity	
Government Identifiers	
National Identification Number	Passport Number

Recipient of the personal data

Recipients of the data Personal data registered is accessible to those organisational units working in security or reception services during the retention period established and for the performance of their duties (monitoring and managing security and safety processes, responding to alarms).
The EPO Technical Department experts, PD 4.4 Advisory Services for the service and updates of the application, and technicians and the external maintenance company technicians have access to the application and its hardware for the performance of the maintenance of those ones.

The data is only used internally by FM security section staff and its external security contractor staff. If other recipients (e.g. Ethics and Compliance, Police, Safety Expert) request access to the personal data this will be individually asked to the Delegated Controller consulting DPO for advice.

Purpose of sharing N/A

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures ACCESS CONTROL SYSTEM Access to the data stored in the access control logs is limited to the administrators of the application. The data will only be accessed upon request and with the permission from the Controller after having obtained favourable advise from the DPO, except in extreme urgency cases in which DPO will be informed. Other users with access to the data such as the external security contractor will only have access to the data stored for the purposes of registering access control, visitor management and number plate registration (parking management). Access to the application and the data stored on it is limited to those with a need to know. Administrators from EPO Security have access to stored log files to monitor compliance and the external security contractor has limited access to operate the application. Access to the application requires the authentication via BIT tools (password/active directory) plus an additional password for the application. All personal data is stored in secure IT applications according to the security standards of EPO. These include: User authentication: All workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication; Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): Separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum; Logical security hardening of systems, equipment and network: 802.1x for network access, encryption of endpoint devices, AV on all devices; Physical protection: EPO access controls, additional access controls to datacentre, policies to lock offices; Transmission and input controls (e.g. audit logging, systems and network monitoring): security monitoring with Splunk; Security incidence response: 24/7 monitoring for incidents, on-call security expert. CARD MANAGEMENT SYSTEM Access to the data stored in the access control logs is limited to the administrators of the application. The data will only be accessed upon request and with the permission from the Controller after having obtained favourable advise from the DPO, except in extreme urgency cases in which DPO will be informed. Other users with access to the data such as the external security contractor will only have access to the data stored for the purposes of registering access to the EPO premises. Access to the application and the data stored on it is limited to those with a need to know. Administrators from EPO Security have access to stored log files to monitor compliance and the external security contractor has limited access to operate the application. Access to the application requires the authentication via BIT tools (password/active directory) plus an additional password for the application. All personal data is stored in secure IT applications according to the security standards of EPO. These include: User authentication: All workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication; Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): Separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum; Logical security hardening of systems, equipment and network: 802.1x for network access, encryption of endpoint devices, AV on all devices; Physical protection: EPO access controls, additional access controls to datacentre, policies to lock offices; Transmission and input controls (e.g. audit logging, systems and network monitoring): security monitoring with Splunk; Security incidence response: 24/7 monitoring for incidents, on-call security expert.

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 161

Name Consultations and assessments of the capacity to work of staff by the EPO Medical Services

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 46 - CIO / BIT

Entity Name - Controller (Entities) DG4 - 42 - People

External processors

Cority / European Patent Office /Technology

External processors	
Name Cority / European Patent Office /Technology	

SAP

External processors	
Name SAP	

Microsoft

External processors	
Name Microsoft	

Microsoft

External processors

Name
Microsoft

GesundArbeiten GmbH

External processors
Name
GesundArbeiten GmbH

Description of the processing

Description This data protection record relates to the processing of personal and medical data for the following purposes

· assess the capacity to work of EPO staff during a medical consultation, and issue a medical opinion when required by EPO regulations
· support staff throughout the process of reintegration into work after a period of illness or an accident
· promote occupational health and wellbeing measures for staff.

Medical consultations to assess the capacity to work for staff by the EPO OHS happen in the following circumstances:
a. Medical consultations when staff are affected by illness or suffer from an accident, in case of sick leave, extended sick leave, incapacity or the transitional period after termination of incapacity.
b. Duty of care medical examination
c. Sick leave verifications including medical examination for staff who accumulated 30 sick leave days within a 12 months period
d. Validation of absences from the place of employment during sick leave

The Office has determined 3 administrative sick leave statuses depending on the number of sick leave days cumulated in a specific period of time:
- sick leave when staff is on sick leave up to 125 working days, either in one unbroken period or in several periods within any rolling period of 18 consecutive months
- extended sick leave when staff is on sick leave up to a total of 250 working days within any rolling period of 36 consecutive months
- incapacity when staff has reached or exceeded the total of 250 working days within any rolling period of 36 consecutive months

OHS receives regularly from BIT the statistics containing the names of staff members that have accumulated 30 or more sick leave days in 1 year or have entered the extended sick leave or incapacity status.

Medical consultations can take place in person or via MS Teams (video) call.

Any medical information (e.g. medical notes, medical reports) is stored in the medical database Cority, divided in OHS Cority and MAU (previously Medical Advisory Unit) Cority. OHS medical and para-medical staff processes medical data using these two databases. Administrative staff (so called front-office staff) have no access to the medical data stored in OHS Cority. OHS personnel have access to the medical database on a need-to-know basis.

There is no exchange of medical information (pathology related) between the EPO medical and para-medical staff and the management, the HRBP or the HR Interlocutors. Medical data in the sense of “administrative data pertaining to health”, for example reintegration plans and confirmation of sick leave, are shared with the respective stakeholders, such as line manager, HRBP/HRI (if participated to the consultation) on a need-to-know basis, e.g. through FIPS /email notification.

The processing is not intended to be used for any automated decision-making, including profiling.

Purpose of Processing Processing of medical data is necessary to provide medical opinions on the capacity to work when required by internal regulations., Processing of medical data is necessary to manage the sick leaves by providing professional support throughout the process of reintegration into work, Processing of medical data is necessary to promote and ensure the health, safety and wellbeing of the employees via the consultations between staff and the EPO Medical Services staff

Data Retention Cority is used since 2006 as main medical database. As of 2016, data are stored only electronically in the EPO medical data base (Cority).
Due to technical constraints, the data are kept permanently in the electronic database.

All data stored in the Outlook e-mail boxes and calendars older than 5 years are deleted.

Data stored in SAP-FIPS are currently stored permanently.

In the event of a formal appeal/litigation, all data held at the time the formal appeal/litigation was initiated will be retained until the proceedings have been closed.

Data subjects and categories of personal data

Employees

General	
Personal Information in SAP	Sensitive Personal Data in SAP
Special Categories of Data in SAP	
Ticketing	
Ticket related data	
Health Data	
Health Data	Medical certificates
Mobility needs	
Contact Information	
Contact Details	Emergency Contact Details
Home Address	Personal Email
Phone Numbers	Working email address
Correspondence	
Personal information provided voluntarily	
Employment Information	
Business Unit Division	Contract Type
Department name and/or number	Hours of Work
Job Group	Job Title Role
Line Reporting Manager	Office Location
Personnel Number	Record of Absence/Time Tracking/Annual Leave

Room Number	Start Date
Personal Identification	
Age	Date of Birth
Disability or Specific Condition	First Name
Full Name	Gender
Marital Status	Nationality

Externals

Contact Information	
Contact Details	Home Address
Personal Email	Phone Numbers
Employment Information	
Job Title Role	

Recipient of the personal data

Recipients of the data Personal and medical data are disclosed on a need-to-know basis to the EPO staff working in Occupational Health Services & Wellbeing.

The following recipients may have access to the categories of personal data including medical data in the sense of "administrative data pertaining to health" and on a need-to-know basis only:
- HR Interlocutors – who receive and process the sick leave certificates and share them on a need-to-know basis with the EPO OHS e.g. in order to inform OHS about extension of the sick leave period and provide any suitable further support to the staff on sick leave.
- Line manager and HRBP – exchange of information with the EPO medical practitioner in charge of the reintegration in order to support the full reintegration of the employee to work.
- Line Manager may have access to the private telephone number of their team to stay in touch in case of long absences for sick leaves reasons.
- Safety experts – in the framework of inquiry, management of any accident or incident occurred at the workplace
- Ergonomics experts – they carry out workplace visits/arrangements triggered by the employee or the OHS staff for a proper ergonomic setup of the work environment
- ServiceDesk – OHS or the ergonomics experts can contact ServiceDesk in order to request to provide a staff member with ergonomic devices not included in the standard supplies.
- BIT – a very limited number of staff of this department provides technical support for the maintenance of the medical databases (Cority)
- In very exceptional cases, Legal Services may have access to personal data for the prevention and management of grievances
- In very exceptional cases, Directorate Ethics and Compliance (DEC) may have access to personal data in the framework of their investigative mandate
- National authorities – a) in very exceptional cases, when the employee has a very serious mental illness that prevents them from taking care of themselves and puts them and/or others at serious risk and any other remedy has been exhausted, the EPO OHS may involve the national social/security services to protect the health, rights and freedoms of staff and/or others; b) when the employee fails to inform their line manager of their absence from work and all attempts made by the line manager and/or the EPO OHS to contact them have been unsuccessful, the EPO may disclose personal information to national public authorities (e.g. police) in the exercise of its duty of care and to protect the health of the staff members.

The following recipients may have access also to the medical data beyond what is mentioned above and, on a need-to-know basis only:

- Emergency physicians / staff of the emergency medical service - in cases where the OHS deem an emergency medical intervention to be necessary and are aware of information essential to the health of the data subject and the data subject is not in a physical/mental condition to provide such information personally (Article 5e DPR)

Personal data may be disclosed to third-party service providers for maintenance and support purposes.

Personal data will only be shared with authorised persons responsible for the necessary processing operations. They will not be used for any other purposes or disclosed to any other recipients.

Purpose of sharing

Transfer

Transfer No

Country where data might be transferred - Processor (Vendors)
Microsoft - United States, SAP - Germany

Transfer to public authority and/or International Organisation	**Reasons for the transfer** Service provider processing data only for Operations/Maintenance purposes
Transfer mechanism(s) The recipient provided appropriate safeguards	**Derogations Art. 10 DPR**

Organisational and security measures

Organisational and security measures Once a year a roles review and logs security audit is carried out. The user manager in SAP–Centre of Excellence department sends to the occupational physician of the EPO OHS the list of users and their respective roles assigned to Cority. The occupational physician must verify and validate the list and roles. The logs security audit is done by the occupational physician directly., For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums)., The access to the medical data base is strictly given only to authorised persons, namely • the EPO medical and para-medical staff, • the System Configurator of the SAP–Centre of Excellence department, • the Emergency User - In urgent cases it is essential that an emergency user exists, in order to intervene in cases of severe malfunction of the system (such as failure of the system, total authorisation blockage or process deadlock). Therefore the emergency user needs the complete Cority access rights. The emergency user has full authorisation allowing the execution of all system and application functions without any authorisation restrictions The access rights allow the above mentioned staff to process and consult only the data for which they are responsible, When face-to-face consultations are not possible or the staff member prefers to have remote consultations, MSTeams is the application used in these cases. Staff is informed not to share messages or documents containing sensitive information during MSTeams (video)calls in accordance with the Office's recommendations (Using Microsoft Cloud tools-http://my.internal.epo.org/portal/private/epo/work/news/?WCM_GLOBAL_CONTEXT=/epo/intranet/work/news/2020/1588753875455_using_cloud_based_tools).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 164

Name Identity Management through AD and Azure AD

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG4 - 46 - CIO / BIT

External processors

Microsoft

External processors	
Name Microsoft	

Microsoft

External processors	
Name Microsoft	

Description of the processing

Description This record encompasses provisioning of user accounts and related user access rules and allocations through the use of Active Directory (AD) and Azure AD as the central repository of user identities.

Two scenarios for provisioning of user accounts are currently in place:
1. Internal (employees and contractors) users are defined in FIPS (master) which is synchronised with On Premise AD using Microsoft Identity Manager (MIM). Subsequently, the On Premise AD is synchronised with Azure AD using Azure AD Connect.

2. Users of national patent offices: the master is Single Access Portal, where users are created, updated and deleted, which is synchronised with On Premise AD using Microsoft Identity Manager (MIM). Subsequently, the On Premise AD is synchronised with Azure AD using Azure AD Connect.

User accounts are subsequently used for authentication and authorisation purposes.

Data Retention User data is kept until flagged inactive in the master (source) system (i.e. FIPS or Single Access Portal) and then kept in both On premise AD and Azure AD for additional 30 days.

At all times during the term of EPO's subscription, EPO has the ability to access, extract and delete the data stored in the applications in scope of this record. Microsoft will retain EPO data that remains stored in the applications in a limited function account for 90 days after expiration or termination of EPO's subscription so that EPO may extract the data.

After the 90-day retention period ends, Microsoft will disable EPO's account and delete the EPO Data and Personal Data within an additional 90 days, unless Microsoft is authorized under the agreement with EPO to retain such data.

For Personal Data in connection with the applications in scope of this record, Microsoft will delete all copies after the business purposes for which the data was collected or transferred have been fulfilled or earlier upon EPO's request, unless authorized under the agreement with EPO to retain such data.

Purpose of Processing Provisioning of user accounts and related user access rules and allocations for authentication and authorisation purposes

Data subjects and categories of personal data

Contractors

Network/application Interaction Data	
Session details	Session metadata
Physical and/or Digital Identifiable Assets	
Digital Certificate	Mobile Device Name
Operating System Version	Workstation's Hostname (Physical or Virtual)
Contact Information	
Mobile Phone Number	Phone Numbers
Working email address	

Building area and site	
Building area and site	
Device Management Data	
Account ID	Azure Active Directory Device ID
Last Logon Time	Tenant ID
Windows ID for Windows Devices	
Browsing Information	
Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
IP Address	
Employment Information	
Active/Inactive Indicator	Business Unit Division
Company Entity	Department name and/or number
Job Title Role	Language preference (of communication)
Line Reporting Manager	Office Location
Personnel Number	Room Number
Personal Identification	
Digital signature	First Name
Gender	Surname
Picture	
User Account Information	
Account Age	Account Password
Membership Permissions	Ownership Permissions
Password Hash	User ID
System Logs	
Audit Logs (a.k.a. Audit Trail)	System-, Application-, Security-related Server Logs

Employees

Network/application Interaction Data

Session details	Session metadata
Physical and/or Digital Identifiable Assets	
Digital Certificate	Mobile Device Name
Operating System Version	Videoconference Room/Equipment Identifier
Workstation's Hostname (Physical or Virtual)	
Contact Information	
Mobile Phone Number	Phone Numbers
Working email address	
Building area and site	
Building area and site	
Device Management Data	
Account ID	Azure Active Directory Device ID
Last Logon Time	Tenant ID
Windows ID for Windows Devices	
Browsing Information	
Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
IP Address	
Employment Information	
Active/Inactive Indicator	Business Unit Division
Department name and/or number	Job Title Role
Language preference (of communication)	Line Reporting Manager
Office Location	Personnel Number
Room Number	
Personal Identification	
Digital signature	First Name
Gender	Surname

Picture	
User Account Information	
Account Age	Account Password
Membership Permissions	Ownership Permissions
Password Hash	User ID
System Logs	
Audit Logs (a.k.a. Audit Trail)	System-, Application-, Security-related Server Logs

Externals

Network/application Interaction Data	
Session details	Session metadata
Contact Information	
Country	Mobile Phone Number
Phone Numbers	Working email address
Employment Information	
Company Entity	
Browsing Information	
Browser type	Browsing Time
IP Address	
Personal Identification	
First Name	Surname
User Account Information	
Account Age	Account Number
Account Password	Membership Permissions
Ownership Permissions	Password Hash
System Logs	
Audit Logs (a.k.a. Audit Trail)	System-, Application-, Security-related Server Logs

Former Employees

Network/application Interaction Data

Session details	Session metadata
Browsing Information	
Browser type	Browsing Time
IP Address	
Personal Identification	
First Name	Surname
User Account Information	
Account Age	Account Password
Membership Permissions	Password Hash
User ID	
System Logs	
Audit Logs (a.k.a. Audit Trail)	System-, Application-, Security-related Server Logs

Recipient of the personal data

Recipients of the data Internal Recipients:

- All EPO staff / contractors
- EPO's staff members from D4623 – IT Security
- Any application which is allowed to interrogate EPO AD/Azure AD to perform user authentication and authorization.

External Recipients:

- Microsoft

If other recipients request access to the personal data, this will be individually asked to the Delegated Controller consulting the DPO for advice.

Purpose of sharing Access to personal data is provided on a need to know basis, only to the necessary categories of personal data depending on the recipient.

Internal Recipients:
- All EPO staff: read access (directly via browser) e.g. via phone book or indirectly via APIs to other Microsoft applications (e.g. Outlook, MS Teams, etc.) to personal data of other EPO staff. EPO staff, including statutory and other internal bodies of the Office, can obtain the personal data of their fellow colleagues through the phone book. This information can be downloaded in bulk via an Excel file, which can then be utilised to, for example, send emails to a large group of recipients.

- EPO's staff members from D4623 – IT Security: AD & Azure AD administrators

- AD/Azure AD personal data are accessed by EPO applications for user authentication/authorization purposes.

External Recipients:
- Microsoft is a recipient for support, maintenance and security services.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors)
Microsoft - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, Protection against malware, login to Azure Active Directory, error analysis, load balancing, diagnostics data and processing for Microsoft's business operations

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures Azure Active Directory is certified according to several security standards (e.g. SOC 1 Type II, SOC 2 Type II), For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums)., For Identity Management systems hosted at EPO premises, the following security measures are in place: All personal data related to Identity management are stored in secure IAM applications according to the security standards of EPO. These include: • User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication; • Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum; • AV on all devices • Physical protection: EPO access controls, additional access controls to datacentre, • Transmission and input controls: audit logging, systems and network monitoring): security monitoring with Splunk; • Security incidence response: 24/7 monitoring for incidents, on-call security expert.

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 165

Name Microsoft Defender for Endpoint

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG4 - 46 - CIO / BIT

External processors

Microsoft

External processors	
Name Microsoft	

Microsoft

External processors	
Name Microsoft	

Description of the processing

Description Microsoft Defender for Endpoint (MDE) is a platform which collects security relevant event data from onboarded endpoints (Windows workstations and Windows servers) and transmits it to an EPO MDE dedicated and segregated cloud tenant for processing and alerting in an automated manner.

BIT PD 4.6 collects MDE security alert-related data from the MDE cloud tenant and stores this on premise in Splunk in an automated manner.

The further processing of personal data within Splunk is described in the dedicated Splunk record.

Purpose of Processing The purpose of the processing is for the Information Security Team to be able to: - prevent security incidents affecting the EPO network and data, such as malware infections - detect and alert to compromises or malicious activity on endpoints in the EPO's infrastructure - investigate and remediate security incidents in the EPO's infrastructure

Data Retention Personal data are stored in logically different places with the following retention rules:
- data stays in a temporary cache area in the endpoint itself, for max 3 days.
- MDE Security alert/incident related data is retained on premise in Splunk for 12 months
- data stay in MDE cloud environment for 180 days, after which it is deleted from MDE cloud tenant
The retention period for the transferred data in the Microsoft Defender for Endpoint Central Unit is no longer than 180 days; after 180 days, data is erased.

Data subjects and categories of personal data

Contractors

Network/application Interaction Data	
Session details	Session metadata
Physical and/or Digital Identifiable Assets	
BIOS Version	Installed Browser Extensions with Indication of their State (Active/Inactive)
Installed Certificates with indication of their Properties	Installed Software Applications
Operating System Version	Processor Type
Vendor Model of Workstation	Workstation Serial Number
Workstation's Hostname (Physical or Virtual)	Workstation's Network Adapter MAC address
Contact Information	
Phone Numbers	Working email address
Device Management Data	
Azure Active Directory Device ID	
Employment Information	
Department name and/or number	Job Title Role
Browsing Information	
Browser type	Browsing Date and Time
Browsing Time	Category
IP Address	Network Interaction History
URL	Website History
Personal Identification	
First Name	Surname

User Account Information	
Account Number	User ID
System Logs	
Audit Logs (a.k.a. Audit Trail)	File data (name, size and/or hash)
Ports	Registry data
Running Processes	System-, Application-, Security-related Server Logs

Employees

Network/application Interaction Data	
Session details	Session metadata
Physical and/or Digital Identifiable Assets	
BIOS Version	Installed Browser Extensions with Indication of their State (Active/Inactive)
Installed Certificates with indication of their Properties	Installed Software Applications
Operating System Version	Processor Type
Vendor Model of Workstation	Workstation Serial Number
Workstation's Hostname (Physical or Virtual)	Workstation's Network Adapter MAC address
Contact Information	
Phone Numbers	Working email address
Device Management Data	
Azure Active Directory Device ID	
Employment Information	
Department name and/or number	Job Title Role
Browsing Information	
Browser type	Browsing Date and Time
Browsing Time	Category
IP Address	Network Interaction History
URL	Website History
Personal Identification	

First Name	Surname
User Account Information	
Account Number	User ID
System Logs	
Audit Logs (a.k.a. Audit Trail)	File data (name, size and/or hash)
Ports	Registry data
Running Processes	System-, Application-, Security-related Server Logs

Externals

Network/application Interaction Data	
Session metadata	
Browsing Information	
Browsing Time	IP Address

Recipient of the personal data

Recipients of the data Recipients of personal data (accessing the data via MDE cloud tenant console on strictly need-to-know basis) are:
- named individuals in EPO 4623 Information Security department
- named individuals having the role Microsoft O365 Global Administrator or the role Microsoft O365 Reader.

Recipients of MDE personal data (stored on EPO premises), on strictly need-to-know basis are:
- members of Dept. 4623 Information Security and Contractors who support Splunk infrastructure and application.

If people or entities other than those mentioned above would request access to MDE personal data, this will be individually asked to the Delegated Controller DP4.6 consulting DPO for advice.

Purpose of sharing Personal data are shared with EPO 4623 Information Security department with the purpose to: - prevent security incidents affecting the EPO network and data, such as malware infections - detect and alert to compromises or malicious activity on endpoints in the EPO's infrastructure - investigate and remediate security incidents in the EPO's infrastructure.

Personal data are shared to named, authorised individuals who have been assigned with the role O365 Global Administrator or O365 Global Reader, in order to let them perform O365 administrative tasks and activities.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors)
Microsoft - United States

Reasons for the transfer Data could be transferred potentially for: protection against malware, login to Azure Active Directory, error analysis, load balancing, diagnostics data, connected experiences, and processing for Microsoft's business operations, Pseudo-anonymised ("Scrubbed") data is sent to central scale unit for threat analytics in the USA.

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO uses role-based access to control access to the MDE console and data. All MDE activities done by any staff with legitimate access are logged and audit trails of such activities is kept., For personal data processed on systems not hosted on EPO premises, the providers processing the personal data have committed in a binding agreement to comply with their data protection obligations under the applicable data protection legal frameworks. The EPO has also carried out a privacy and security risk assessment. Any personal data in transit over public networks between the EPO and Microsoft, or between Microsoft data centres is encrypted by default. Personal data as part of any data that are provided to Microsoft by, or on behalf of, EPO through use of the Microsoft Defender for Endpoint is encrypted at rest. Regarding the implementation of the encryption, Microsoft uses state of the art encryption technologies. Furthermore, Microsoft employs least privilege access mechanisms to control access to personal data which are part of data that are provided to Microsoft by EPO and role-based access controls are employed to ensure that access to such personal data required for service operations is for an appropriate purpose and approved with management oversight. For Microsoft services any required access by Microsoft is for a limited time. Microsoft implements and maintains multiple security measures for the protection of personal data as part of any data that are provided to Microsoft by EPO through use of the Microsoft Defender for Endpoint, which encompass the following: organisation of information security (e.g., security ownership, security roles and responsibilities, risk management program), asset management (e.g. asset inventory and asset handling), human resources security (e.g. security training), physical and environmental security (e.g. physical access to facilities, physical access to components, protection from disruptions, component disposal), communications and operations management controls (e.g. operational policy, data recovery procedures, anti-malware controls, event logging), access control measures (e.g. access policy, access authorisation, least privilege, integrity and confidentiality, authentication, network design), information security incident management (e.g. incident response process, service monitoring) and business continuity management. Microsoft also implements and maintain appropriate technical and organisational measures for protection of any other personal data distinct from the one described above, which are described in Microsoft Security Policy. Microsoft Defender for Endpoint has been configured to preserve the confidentiality of the information by employing the measures listed above. In addition, anonymous access is not authorised. Microsoft Defender for Endpoint is certified in several security standards, including ISO27001, SOC1 Type II, SOC2 Type II and ISO27018 Code of Practice for Protecting Personal Data in the Cloud and complies with the requirements set forth in ISO 27002. Microsoft conducts annual audits of the security of the computers, computing environment, and physical data centres that it uses in processing of personal data. The audits are performed by independent, third-party auditors according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework. Personal data is stored in the EU according to the application configuration implemented by the EPO. It may, however, be made available to subprocessors in other countries, depending on the requirements for maintenance, support or operation of cloud-hosted services, and the availability of this expertise. If access is granted, it is always temporarily and only to the data required for the specific maintenance, support or operation procedure being carried out. The following safeguards are implemented: • In all transfers to third countries, Microsoft uses EU Standard Contract Clauses for data transfer with its sub-processors. • Microsoft requires subprocessors to join the Microsoft Supplier Security and Privacy Assurance Program. This programme is designed to standardise and strengthen data handling practices, and to ensure that supplier business processes and systems are consistent with those of Microsoft.

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 166

Name Accident reporting

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 44 - General Administration

Entity Name - Controller (Entities) DG4 - 44 - General Administration

External processors

Microsoft

External processors	
Name Microsoft	

DEKRA

External processors	
Name DEKRA	

Description of the processing

Description Accident registration procedure for EPO employees, visitors and contractors:

1. The staff member suffering from an accident (called victim hereinafter) during the course of its duties or in relation to its duties needs to fill out the accident registration form (ARF) via an online form in MyFIPS along with a detailed description of the incident's circumstances and some information on its health effects .
2. The contractor's staff suffering from an accident during the course of his/ her duties or in relation to his/ her duties on EPO premises needs to inform the EPO contract manager via his/ her manager about the details of the accident. The EPO contract manager fills out the accident registration form (ARF) based on the information provided by the contractor's manager.
3. The visitor suffering from an accident during the course of his/ her visit needs to inform the respective EPO contact person who fills out the accident registration form (ARF) on behalf of the visitor.4. The ARF is submitted automatically via email to the EPO Health & Safety Service desk (healthandsafety@epo.org) that store it in the medical database and forwarded to the EPO Health Services and to the OSE (Occupational Safety Expert).
4. The ARF has to be submitted by EPO staff within 10 days following the incident. In case that the 'victim' is not in physical condition to complete the form the victim's line manager initiates the form. In case the visitor or the manager of the contractor cannot receive sufficient background information he/ she initiates the form with the available data within 24h following the accident. Detailed information is provided by the victim him/herself as soon as possible.
5. The OSEs register the incident manually on a database kept in the OSE's environment and initiates the investigation process, which looks only at the circumstances of the incident and does not disclose any personal data information.
6. EPO Health Services and/or the OSE may get in touch with the victim to offer support if needed.
7. In case of claim for medical expenses over and above the medical insurance coverage, the EPO Health Services will assess the claim.
8. The personal data related to the accident are kept for 5 years so to provide a record.

Internal processor:
- Health Services/ EPO Occupational Health Physician – for any medical assessment / support if necessary

For all the sites the procedures are followed by the external occupational safety experts. The EPO internal Safety experts are supervising and monitoring the procedure.

Personal data and information are processed and stored in the EPO IT environment only.

Data Retention Accident Reports are submitted through SAP-MyFips and received per email. They are stored locally in OpenText for a maximum of 5 years. There are manually deleted until an automatic deletion is programmed.

In case of an accident investigation is launched the report will be kept and the personal data anonymised after 5 years

Purpose of Processing Processing of personal data is necessary to: • promote and ensure the health, safety and wellbeing of EPO staff at the workplace; • manage any deficiencies and malfunctions so to avoid re-occurrence of incidents; • improve the health and safety level within the Office. • improve emergency response. The processing is not intended to be used for any automated decision making, including profiling.

Data subjects and categories of personal data

Contractors

Health Data
Health Data

Contact Information	
Phone Numbers	Working email address
Building area and site	
Building area and site	
Personal Identification	
Age	Disability or Specific Condition
Full Name	Gender

Employees

Health Data	
Health Data	
Contact Information	
Contact Details	Phone Numbers
Working email address	
Employment Information	
Job Title Role	Personnel Number
Record of Absence/Time Tracking/Annual Leave	
Personal Identification	
Age	Disability or Specific Condition
Full Name	Gender

Externals

Contact Information	
Personal Email	Phone Numbers
Building area and site	
Building area and site	
Personal Identification	
Age	Disability or Specific Condition
Full Name	Gender

Recipient of the personal data

Recipients of the data The following recipients may have access to the personal data only on a need-to-know basis:

- EPO Health Services – they support and cooperate with the Safety Experts when required and are involved in the procedure for the additional reimbursement of medical expenses related to occupational accidents.
- External safety experts (DEKRA)
- Security
- Legal services

Purpose of sharing Health Services: for further processing of the accident (medical treatment, reimbursement...)
DEKRA: for registering purposes.
Security: in case of an investigation where only the name of the data subject could be shared.
Legal service: potentially in case of a liability / litigation

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 167

Name Medical certificates/consultancy registration process

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 46 - CIO / BIT, DG4 - 423 - HR Essential Services

Entity Name - Controller (Entities) DG4 - 422 - People Engagement and Partnership

External processors

SAP

External processors	
Name SAP	

Microsoft

External processors	
Name Microsoft	

Microsoft

External processors	
Name Microsoft	

Description of the processing

Description All staff members are required to be certified sick by a medical practitioner or by the EPO Medical Services or in exceptional cases to consult their treating doctor as from the fourth (working) day of sick leave accrued in any calendar year as lined out in Art. 62a ServRegs and Circ. 367.

You as staff member are required to notify your line manager by phone or by email of the inability to perform your duties.
When returning to work you will use MyFIPS portal in order to
-register the date of your return to work via the "Return from sick leave" form
-select one of the options chosen to certify your absence (i.e. medical certificate issued by your treating physician or by the EPO medical services, name & address of the doctor consulted)
-submit the relevant document(s) by uploading them in MyFIPS directly.

The medical certificate should state:
- Your name, date of birth, country, home address
- The date of issue of the certificate
- The name, signature address and medical specialisation of the doctor who issues the certificate
- The start date and estimated end date of the absence for health reasons
- No diagnosis is to be included.

No medical details are to be included in the medical certificate. If they choose to send it anyway (e.g. if they send the version of the medical certificate including the diagnosis code, which they should not, because there is a specific version for employers), it is ignored by HR interlocutors (referred to as HRIs in the following text) and deleted after the retention period.

You must keep the original of the medical certificates for four years.

Reduced working time schedules are issues by OHS and send via email to the HR Ticketing System. The re-integration plans are then entered by the HRIs.

Only the HRIs may have access to the medical certificate on a need-to-know basis.

Before 01.04.2023, the medical certificate and consultancy registration process required the processing of emails and the certificates were sent either electronically (as attachment to the email and in this cases they were kept in a "recorded" subfolder of the HRI common inbox) or by post (in this case they were stored in a locked cupboard).

Data certifying the sick leave are retained for 4 years and then deleted/destroyed.

Only the records in SAP remain (e.g. certified sick leave period with start and end date).

Data can be used for anonymized statistics purposes.

EPO medical services may request on a need-to-know basis copy of sick leave certificates of staff in long term sick leave in order to be promptly informed about extension of the sick leave period and therefore provide any suitable further support for follow-up of the reintegration process.

HRIs are bound by confidentiality and also sign a confidentiality and data protection information sheet (see template attach).

Purpose of Processing Produce anonymized statistics, Ensure compliance with the sick leave certificate regulations (Art. 62a ServRegs, Circ. 367)

Data Retention Data certifying the sick leave are retained for 4 years and then deleted/destroyed.

Currently the entries about the certified periods remain in SAP-FIPS permanently. By 2024, an automatic deletion function should be implemented

Data subjects and categories of personal data

Externals

Contact Information	
Contact Details	Country
Home Address	Phone Numbers
Employment Information	
Job Title Role	
Personal Identification	
Full Name	

Employees

Health Data	
Health Data	Medical certificates
Name and address of treating physician	
Contact Information	
Country	Home Address
Personal Identification	
Date of Birth	First Name
Full Name	Surname

Recipient of the personal data

Recipients of the data The HRI team have access to the data for the administration of the sick leave certificates of the employees.
EPO medical services may request on a need-to-know basis copy of sick leave certificates of staff in long term sick leave in order to be promptly informed about extension of the sick leave period and therefore provide any suitable further support for follow-up of the reintegration process.
Line manager may be informed about the certified period of absence but they do not get copy of the certificates.
BIT may provide technical support

Purpose of sharing

Transfer

Transfer Yes

Country where data might be transferred - Processor (Vendors) SAP - Germany, Microsoft - United States

Transfer to public authority and/or International Organisation

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Transfer mechanism(s) The recipient provided appropriate safeguards

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 175

Name Employee Assistance Programme (EAP)

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG4 - 423 - HR Essential Services

External processors

LifeWorks

External processors	
Name LifeWorks	

AWP Health & Life Services Limited

External processors	
Name AWP Health & Life Services Limited	

Telus Health

External processors	
Name Telus Health	

Description of the processing

Description Staff member or dependent may contact the EAP Care Access Centre for confidential short-term counselling to solve personal or work-related problems, pressures and stress situations.

In particular, assistance is provided for:
• Coping with isolation and loneliness
• Adapting across cultures
• Identifying and coping with culture shock
• Addressing the personal impact of the relocation
• Dealing with stress, anxiety, and depression
• Addressing alcohol and drug misuse
• Resolving marital and relationship difficulties
• Finding solutions for work-related issues
• Offering advice and referrals for work-life issues such as family support / parenting / elder care
• Accessing crisis and trauma support
• Address legal or financial issues
• Working towards life goals
• Strengthening relationships
• Improving communication

The Procedure can be described as follows.

- The first contact is made by phone .
- The staff members/dependents have to provide the name of the EPO in order to identify the employer offering this service.
- They are free to decide to remain anonymous by using a pseudonym.
- Email address and / or phone number are needed by the provider as contact data.
- Other personal data and information might be asked according to the kind of support that is provided. These additional personal data are always taken for the purpose of providing the specific support the person requests.
- After a preliminary case assessment, the EAP Care Access Centre identifies a specialist with whom the staff member/dependent can have approximately 6 support sessions over the telephone, online or in person.
- If the staff members/dependents need more specialised or long-term support, the service provider will help them select an appropriate specialist or service.
- Once a case is closed, the staff member/dependent is asked by the provider to evaluate the service via an anonymous survey.
-Quarterly and annually the D4225 Wellbeing and Engagement receive aggregated data reports by the service provider.
- In addition the EAP offers an online platform, called LifeWorks, that can be accessed via an app or PC. Credentials to access this platform are EPO bound, not individual.
- The platform provides information about health and wellbeing and offers the possibility to contact the EAP care access centre.

Information relating to participation in the EAP is strictly confidential. No information is shared with anyone without informed, voluntary and written consent. Only in order to protect the vital interest of the staff/dependent or third parties, the external service provider can, and has to, inform the national authorities and disclose personal data.

For the vast majority the personal data processed by AWP Health & Life Services Limited (Allianz) and Telus Health (formerly LifeWorks and LifeWorks war formerly Morneau Shepell), the EPO is not the controller. In principle, AWP Health & Life Services Limited and Telus Health are the controllers of the personal data provided directly by the users of the Services.

The contract with will end on 31.01.2025. In Q1 2024 the Delegated Controller will start a new tender procedure and the relevant risk assessments will be carried out.

Purpose of Processing - Providing staff members and their dependants with free access to psychosocial support and counselling if there is a need to help reconcile work and home life. - Making sure the right support is given and the needs are addressed accordingly by receiving the relevant and correct data from the person, Access to the online platform

Data Retention This information is missing pending the finalization of the DPA (Data Processing Agreement).

Data subjects and categories of personal data

Employees

Health Data	
Health Data	
Contact Information	
Personal Email	Phone Numbers
Employment Information	
Company Entity	

Externals

Health Data	
Health Data	
Contact Information	
Personal Email	Phone Numbers
Employment Information	
Company Entity	

Recipient of the personal data

Recipients of the data Within EPO
Only aggregated data or the anonymised surveys are shared with D4.2.3, D4.2.2, PD4.2, VP4, President, COHSEC.

Outside the EPO
Telus Health - (the Sub-Processor) is the party that deals with all the processing of personal data and it is the only party that has access to raw personal data.

Allianz - (the Data Processor) only receives the data EPO receives i.e. results of aggregated anonymised reports of service satisfaction and the "Utilisation Report".

Purpose of sharing

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer The external processor is based in the UK

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures	For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 177

Name Physiotherapy service

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG4 - 423 - HR Essential Services

External processors

High Five Health Promotion B.V

External processors	
Name High Five Health Promotion B.V	

B&R Health Management

External processors	
Name B&R Health Management	

Description of the processing

Description The service:
- The Physiotherapy Service is provided exclusively by external service providers, namely High-Five in Munich and B&R Health Management in Netherlands.
- The service providers and all the sub-processors involved for the purpose of physiotherapy services are located in EEA and therefore bound by the EU data protection regulation.
-Physiotherapy services are offered to all EPO staff-members

The procedure:
- When a staff member is interested, the staff member contacts the Physiotherapist providers directly by finding on the intranet the contact details of the Physiotherapists and also information about the tools they need to use to book an appointment.
- Appointments can scheduled by phone, e-mail, direct contact or via the online booking tool.
- On the day of the appointment, the staff member will be invited to share with the Physiotherapist the necessary personal and medical data needed for the service.
- All the personal data are shared by the staff-member that requests the service.
- All these data are stored as medical files in the databases the providers use.

Data storage and retention:

- The external service providers use their own applications only not the ones of the Office so EPO has no access to these tools.
- All IT applications used by the service providers for the provision of the service (e.g. scheduling, invoicing, maintaining the patient history for the provision of the physiotherapy services, complying with national regulations) are stored in data centres located in the EEA.
- Paper files containing medical data (e.g. doctor's prescription, medical notes) are stored in locked cupboards in the physiotherapy rooms and the keys are available only to the physiotherapists.
- Usually what the physiotherapists put on paper is only their personal schedules. The medical data is stored in the online tools the service providers use so medical data are not stored on paper.

The external service providers provide a yearly anonymous report that shows the most common injuries and what are the most common reasons the staff members contact the physiotherapists.

The EPO does not receive any personal or medical information on its staff from the external service provider.

Data Retention Payment information and medical files are retained according to the applicable national regulations. During this retention period data will not be anonymised nor pseudonymised.
After this retention time the data will be deleted.

Purpose of Processing Provide anonymized report to D423, Offer preventive physiotherapy advice as well as physiotherapy treatment for the staff members. Make sure the service is provided effectively and it is easy to reach.

Data subjects and categories of personal data

Employees

Health Data	
Health Data	
Contact Information	
Contact Details	Home Address
Mobile Phone Number	Personal Email

Phone Numbers	Working email address
Building area and site	
Building area and site	
Correspondence	
Additional Information which might be provided in the course of exchanges	Personal information provided voluntarily
Financial	
Bank Account Information	
Employment Information	
Weight	
Personal Identification	
Age	Date of Birth
Full Name	Gender
Height	Nationality

Externals

Contact Information	
Contact Details	

Recipient of the personal data

Recipients of the data External providers and their sub-processors for the administration and management of the services (e.g. scheduling, invoicing, maintaining the patient history for the provision of the physiotherapy services, complying with national regulations)

D423 receives only anonymized aggregated data for analysis purposes.

The data are not used for any other purposes nor disclosed to any other recipient.

Purpose of sharing

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures	For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 178

Name Registration of Munich staff's children in crèches subsidised by the Office

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG4 - 423 - HR Essential Services

External processors

AWO-Pschorr

External processors	
Name AWO-Pschorr	

Merlin

External processors	
Name Merlin	

KiTa Haar

External processors	
Name KiTa Haar	

AWO-Isar

External processors

Name
AWO-Isar

Description of the processing

Description In-house crèche
Personal data are processed in order for Munich staff to apply for a place in an in-house crèche via a dedicated online registration tool accessible from the EPO intranet.

Once the EPO staff members submits their application, they are automatically registered in the registration tool managed by D4233 under the status “inscribed” and an automatic ‘receipt of request’ confirmation is sent via Outlook to the staff member.
D4233 Expatriation and Social Services revises the request, i.e., confirms directly with the in-house crèche whether there is a vacancy.

In case there are no vacancies, no communication is sent to the staff member. When a place becomes available however, D4233 sends an offer by e-mail to the staff member concerned and includes the crèche in Cc. The EPO does not transmit personal data included by the staff member on the dedicated tool to the crèche – only name and surname of the parent(s) and child and birthday of the child are included in the e-mail. The staff member is instructed in said e-mail to contact the crèche directly in order to proceed with the enrolment of their child.

In case the staff member accepts the offer, they are to inform D4233 who, upon such confirmation, will change the status in the registration tool from “inscribed” to “under offer”.

In case the staff member refuses the offer, they are to inform D4233. The status in the registration tool will be changed by D4233 from “under offer” to “cancel”.

In case the staff members contracts with the crèche, the staff member and/or the crèche informs D4233 when they accept the place. The status change is then changed by D4233 in the registration tool from “under offer” to “placed”.

In case of terminations, the crèche sends a termination confirmation to the staff members with D4233 in Cc. Upon such confirmation, D4233 changes the staff member’s status in the registration tool from “place” to “closed”.

The crèche sends D4233 regular updates on occupancy and D4233 updates the registration tool accordingly. The updates from the crèches are word or excel files. These are deleted 1 year after the end of the crèche year

External crèche Kita Haar
The registration process runs outside the registration tool. The parents contact D4233 directly in case of interest in the external crèche. D4233 informs KiTa Haar by email providing name and surname of the staff member and child and announces the registration. The parents then contact the KiTa Haar directly and conclude the contract. The EPO pays a place fee.

The registrations are recorded in an excel list, which is deleted 1 year after the termination of the childcare.

Purpose of Processing The purpose is to process staff members’ requests for a place in the Munich in-house/external crèches and to allocate the places to the eligible persons.

Data Retention Data stored in the registration toll are deleted after 1 year the child has left the crèche.

Emails stored in Outlook for the processing of the requests are deleted after 1 years from the date on which the email is sent.

Data subjects and categories of personal data

Employees

Contact Information	
Contact Details	Home Address
Phone Numbers	Working email address
Family Information	
Children's Names	Child's birthday
Spouse's name	

Externals

Contact Information	
Contact Details	Working email address

Recipient of the personal data

Recipients of the data AWO-Isar
AWO-Pschorr
Merlin
KiTa Haar

BIT might have access to the data for technical support or/and IT service maintenance

Statistics could possibly be requested by management, but these would only contain anonymised data.

Purpose of sharing Allocation of crèche places to registered families/children

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network	

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 179

Name Consultation with the Ombuds Office - external clients

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG0 - 045 - Internal Audit and Professional Standards - Ombuds Office

Description of the processing

Description - Client raises a matter with the Ombuds Office.
- In-take of the case data: The confidential treatment of the data provided by the client is also explained in the DPS as follows:

"When you contact the Ombuds Office, your matter will be treated in the strictest of confidence. Your data will be shared confidentially with the appropriate EPO managers, who will receive the minimum information essential to deal with your matter. Should the Ombuds Office consider it necessary to share your personal data with any other EPO staff involved in your matter, it will do so only with your express agreement.

Once your matter is closed, all personal data, including any reference to your organisation or affiliation or to the applicant you are representing, will be deleted. You can close your matter at any time, in which case all personal data, including any reference to your organisation or affiliation or to the applicant you are representing, will be deleted.

The Ombuds Office will keep an anonymous record of reported matters to enable it to identify trends or systemic issues. Its reports will not contain any details relating to personal data or to organisations or affiliations.

In exceptional cases, where the Ombuds Office considers information shared with it to indicate an imminent risk of serious harm to an individual or an illegal activity, it will share this information with relevant EPO managers to enable them to take appropriate action. If your matter relates to an integrity issue, such as fraud, corruption or other irregular activities, you should report it to the EPO department responsible for ensuring compliance at investigations@epo.org or at + 49 89 2399 1577.

You may inform the Ombuds Office at any time that you do not wish to continue the procedure with the Ombuds Office. In this case, your personal data, including any reference to your organisation or affiliation or to the applicant you are representing, will be deleted and any other data you have provided will be anonymised.

Please be reassured that your personal data will be processed solely for the above-mentioned purposes. In addition, the processing is not intended to be used for any automated decision making, including profiling. Your personal data will not be transferred to recipients outside the EPO."

Data Retention Any personal data, including reference to organisation, affiliation or representation, collected during a consultation with a client will be deleted upon confirmation from the client that the matter is closed.

Anonymised non-case related data will be retained and used to generate systemic and trend data for reporting and general quality improvement actions.

Purpose of Processing Personal data are processed with the purpose of assisting that the client in getting their matter back on track when the regular formal channels have been unable to resolve the matter to their satisfaction. The Ombuds Office will also maintain an anonymous record of reported matters so that it can identify trends or systemic issues. Its reports will not contain any details relating to personal data or organisations or affiliations.

Data subjects and categories of personal data

Employees

General	
Any other information	Assessment and legal opinions
Phone Call Information	
Called Phone Number	Caller's Phone Number

Phone Call Date and/or Time	Phone Call Duration
Phone Call Interaction History	Phone Calling History
Contact Information	
Contact Details	Mobile Phone Number
Personal Email	Phone Numbers
Private Phone Number	Working email address
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Patent Process Related Data	
Personal data potentially included within the content of patent procedure related information and publications	
Employment Information	
Assessment and legal opinions	Business Unit Division
Department name and/or number	Job Title Role
Office Location	
Personal Identification	
Digital signature	First Name
Full Name	Surname

Externals

General	
Any other information	User association
Phone Call Information	
Called Phone Number	Caller's Phone Number
Phone Call Date and/or Time	Phone Call Duration
Phone Call Interaction History	Phone Calling History
Contact Information	
Contact Details	Home Address

Mobile Phone Number	Personal Email
Phone Numbers	Working email address
Professional Experience & Affiliations	
Affiliation	Professional Memberships
Representation in EPO's Patent Granting Process	
Affiliation to Association of professional representatives	Role in the Patent Grant Procedure
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Patent Process Related Data	
Personal data potentially included within the content of patent procedure related information and publications	
Employment Information	
Business Unit Division	Company Entity
Department name and/or number	Job Title Role
Office Location	
Personal Identification	
Digital signature	First Name
Full Name	Surname
Signature	

Recipient of the personal data

Recipients of the data When you contact the Ombuds Office, your matter will be treated in the strictest of confidence. Your data will be shared confidentially with the appropriate EPO managers, who will receive the minimum information essential to deal with your matter. Should the Ombuds Office consider it necessary to share your personal data with any other EPO staff involved in your matter, it will do so only with your express agreement.

Purpose of sharing cf. comments to 1.6

When you contact the Ombuds Office, your matter will be treated in the strictest of confidence. Your data will be shared confidentially with the appropriate EPO managers, who will receive the minimum information essential to deal with your matter. Should the Ombuds Office consider it necessary to share your personal data with any other EPO staff involved in your matter, it will do so only with your express agreement.

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer

Transfer mechanism(s)	Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network	

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 180

Name Personal Evacuation Emergency Plan (PEEP)

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 44 - General Administration

Entity Name - Controller (Entities) DG4 - 44 - General Administration

External processors

Microsoft

External processors	
Name Microsoft	

External contractor DEKRA

External processors	
Name External contractor DEKRA	

Security Services Contractor at all EPO sites

External processors	
Name Security Services Contractor at all EPO sites	

Description of the processing

Description Occupational Safety Experts' role is to advise and support EPO Management in fulfilling the manager's duty of care for staff. This includes drawing up the Personal Evacuation Emergency Plan (PEEP) to support persons with disability that would need assistance in case of evacuation.

For all EPO sites this service is provided by external occupational safety experts (deputies) under the supervision of the internal safety expert team.

In all cases the data and information is processed and stored in the EPO IT environment.

To establish PEEP the following processing operations take place:
1. Staff: People with a temporary or permanent disability can contact Occupational Health and Safety service desk (healthandsafety@epo.org) and requests a PEEP.
2. The person with the disability provides consent to share the PEEP data with Physical Security and Occupational Health by means of signing the PEEP document. In addition, the line manager and/or specific people may be added as receivers of the PEEP upon request from the person with the disability.
3. Data required for staff PEEPs are name, room number / location in the building and E-mail address of those requiring assistance. In addition, the name and E-mail address of the line manager and/or specific people may be added if required.
4. PEEPs of staff are kept until a) the staff member requests deletion, b) the staff member leaves the EPO, c) the staff member retires, d) the disability is no longer relevant or e) no response is given during a validity check. Occupational Safety evaluates the validity of PEEPs annually.
5. Visitors: The EPO person who invited the visitor with disability can request a PEEP on behalf of the visitor, provided written consent was given. This should be done by contacting Occupational Health and Safety service desk (healthandsafety@epo.org) before the visit, and providing the necessary information required for the PEEP.
6. Visitor PEEPs are shared with Physical Security, Occupational Health and the event organiser(s) on a need-to-know bases.
7. It is the responsibility of the EPO person who invited the visitor with a disability to fully inform them of the process and with whom the data is shared internally.
8. Personal data required for a visitor PEEP are name and telephone number of those requiring assistance.
9. Visitor PEEPs are deleted by written request of the visitor and/or upon completion of the visit.

Purpose of Processing Processing of some personal data is necessary to: • ensure the safety of EPO staff and visitors with disabilities • provide specific support to colleagues with disability issues in case of an emergency • To support and improve the emergency response

Data Retention For EPO employees:
Validity of the PEEP is checked annually, if no longer valid, the data will be removed. For EPO employees, this means a) the disability is gone, b) the individual retired or has left the Office c) the individual requests deletion of data.

For visitors:
The personal data is deleted as soon as the visit ends upon request of the visitors for whom a PEEP has been established.

Data is stored in the EPO servers, in MS Team database (only files with restricted access), in EPO OT and Outlook.

Data subjects and categories of personal data

Employees

Building area and site

Building area and site	
Employment Information	
Office Location	Room Number
Personal Identification	
Full Name	

Externals

Building area and site	
Building area and site	
Employment Information	
Office Location	
Personal Identification	
Full Name	

Recipient of the personal data

Recipients of the data The following recipients may have access to the data only on a need-to-know basis:
• Occupational Health – the data is shared for information (safety report)
• Line manager of the staff concerned for the follow up of actions in case the PEEP is activated and with the consent of the individual
• Restricted number of colleagues of a disabled employee, in some PEEP cases in order to support the emergency response process and with the consent of the individual
• Operations Office/Physical Security
The data is shared with the consent of the person with disability.

Purpose of sharing For the safety of the person with disability and as

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 182

Name Disposal of e-waste

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG4 - 46 - CIO / BIT

External processors

PlanBit

External processors	
Name PlanBit	

Description of the processing

Description In the context of the EPO's environmental sustainability goals and in particular the EPO's target to be carbon neutral by 2030, the eWaste (ITAD) service for ICT assets and electronics has been put in place to provide a single point of disposal service for any brand and multi types of ICT asset owned by the EPO, managing ICT assets disposals in an ethical and sustainable way and contributing, amongst others, to end-of-life responsible recycling and upcycling and reduction of e-waste and thus contributing to a more circular business economy.

In that context, personal data is processed as follows:

1) For the management of the contract, processing of personal data will be limited to the contact details (Name/Surname; work e-mail; work phone numbers) of the EPO staff authorised to manage the contract

2) For the performance of the contract, in particular the sanitisation of any data bearing devices, personal data processing (i.e. destruction or data erasure / complete and irreversible deletion or data wiping)) could theoretically include any kind of personal data stored on the media.
The service therefore provides for an end-to-end tracing of the hardware media and data, including GPS tracking from the moment equipment is collected at the EPO, serialized recording upon arrival at the facility, detailed traceability for data bearing devices, detailed end reports for all devices and traceability after processing (reuse or recycling).
Deletion is done according to the NIST 800-88 standard.
The deletion processes are automated, i.e. the technicians don't access the personal data in order to delete it.
If deletion attempts are unsuccessful, the data media will be built out and shredded

Data Retention 1) For the management of the contract, data will be retained for the duration of the contract.
2) For the performance of the contract, no personal data will be retained (as the purpose is to erase / delete the data). Certificates of data removal will be kept for 5 years (no personal data in scope here).

Purpose of Processing 1) Management of the contract with PlanBit.,
2) Performance of the contract, in particular the sanitisation of the information media (i.e. destruction or data erasure / complete and irreversible deletion or data wiping).

Data subjects and categories of personal data

Contractors

Applications' Log	
SAP Logs	
Social	
Social Media Account	Social Media Contact
Social Media History	
Sensory and Electronic Information	
Audio Information	Electronic Information
Thermal Information	Time stamps from their access to the buildings
Visual Information	
Building area and site	

Building area and site	
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name
Gender	Height
Surname	Marital Status
Nationality	Picture
Racial or Ethnic Origin	Religion/Religious Beliefs
Sexual Orientation	Signature
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
General	
Assessment and legal opinions	
Workplace Welfare	
Records of Personal Properties	
Contact Information	
Contact Details	Emergency Contact Details
Home Address	Personal Email
Phone Numbers	Previous Residence Address
Teleworking address	Working email address
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data

IDP	Instructor related data
Learning external events	Learning history
Learning plan	Social learning inputs
Correspondence	
Personal information provided voluntarily	
Health Insurance Information	
Insurance Policy Information	Unique Identifier for Subscriber
Ticketing	
Ticket related data	
Biometric	
Body temperature	Facial Recognition
Fingerprint	Voice Recognition
Background Checks	
Criminal History	Criminal Records
Drug Test Results	Reference or Background Checks
Employment Information	
Appeals Records Information	Assessment and legal opinions
Benefits and Entitlements Data	Business Unit Division
Company Entity	Contract Type
Corporate Credit or Debit Card Numbers	Department name and/or number
Disciplinary Action	End Date
End Date and Reason for Termination	EPO access badge number
Exit Interview and Comments	Grade
Grievances and Complaints	Hours of Work
Job Application Details	Job Title Role
Language preference (of communication)	Line Reporting Manager
Military Status	Office Location

Performance Rating	Personnel Number
Previous Work History	Record of Absence/Time Tracking/Annual Leave
Room Number	Salary
Start Date	Weight
Unknown	
EPO badge validity	Price list for discounts
Geolocation	
Geolocation Information	
Network/application Interaction Data	
Session details	
Health Data	
Health Data	
Professional Experience & Affiliations	
CV	Political Affiliation and Activities
Professional Memberships	Qualifications Certifications
Trade Union Membership	
Financial	
Bank Account Information	Bank Account Number
Bank Statements	Bonus Payments
Compensation Data	Credit Card Number
Credit History	Debit Card Number
Fund Reservation Requests	Information on home loans
Insurance Information	Routing Number
Browsing Information	
Browsing Time	Cookie Information
IP Address	Network Interaction History
Website History	
User Account Information	

Account Age	Account Number
Account Password	Password
User ID	
Government Identifiers	
Driving Licence Number	National Identification Number
National Identity Card Details	Passport Number
Social Security Number	

Employees

Applications' Log	
SAP Logs	
Social	
Social Media Account	Social Media Contact
Social Media History	
Sensory and Electronic Information	
Audio Information	Electronic Information
Thermal Information	Time stamps from their access to the buildings
Visual Information	
Building area and site	
Building area and site	
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name
Gender	Height

Surname	Marital Status
Nationality	Picture
Racial or Ethnic Origin	Religion/Religious Beliefs
Sexual Orientation	Signature
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
General	
Assessment and legal opinions	
Workplace Welfare	
Records of Personal Properties	
Contact Information	
Contact Details	Emergency Contact Details
Home Address	Home Leave Address
Personal Email	Phone Numbers
Previous Residence Address	Teleworking address
Working email address	
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
Diagnostic tools' results	IDP
Instructor related data	Learning external events
Learning history	Learning plan
Ratings	Social learning inputs
Correspondence	
Personal information provided voluntarily	
Health Insurance Information	
Insurance Policy Information	Unique Identifier for Subscriber
Ticketing	

Ticket related data	
Biometric	
Body temperature	Facial Recognition
Fingerprint	Voice Recognition
Background Checks	
Criminal History	Criminal Records
Drug Test Results	Reference or Background Checks
Employment Information	
Appeals Records Information	Assessment and legal opinions
Benefits and Entitlements Data	Business Unit Division
Company Entity	Contract Type
Corporate Credit or Debit Card Numbers	Department name and/or number
Disciplinary Action	End Date
End Date and Reason for Termination	EPO access badge number
Exit Interview and Comments	Grade
Grievances and Complaints	Hours of Work
Job Application Details	Job Title Role
Language preference (of communication)	Line Reporting Manager
Military Status	Office Location
Performance Rating	Personnel Number
Previous Work History	Record of Absence/Time Tracking/Annual Leave
Room Number	Salary
Start Date	Weight
Unknown	
EPO badge validity	Price list for discounts
Geolocation	

Geolocation Information	
Network/application Interaction Data	
Session details	
Health Data	
Health Data	
Professional Experience & Affiliations	
CV	Political Affiliation and Activities
Professional Memberships	Qualifications Certifications
Trade Union Membership	
Family Information	
Children's Names	Child's birthday
Parents' Names	Spouse's information
Spouse's name	
Financial	
Bank Account Information	Bank Account Number
Bank Statements	Bonus Payments
Compensation Data	Credit Card Number
Credit History	Debit Card Number
Fund Reservation Requests	Information on home loans
Insurance Information	Routing Number
Browsing Information	
Browsing Time	Cookie Information
IP Address	Network Interaction History
Website History	
User Account Information	
Account Age	Account Number
Account Password	Password

User ID	
Government Identifiers	
Driving Licence Number	National Identification Number
National Identity Card Details	Passport Number
Social Security Number	

Externals

Applications' Log	
SAP Logs	
Social	
Social Media Account	Social Media Contact
Ticketing	
Ticket related data	
Sensory and Electronic Information	
Audio Information	Electronic Information
Time stamps from their access to the buildings	Visual Information
Building area and site	
Building area and site	
Biometric	
Facial Recognition	Voice Recognition
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Employment Information	
Business Unit Division	Company Entity
Contract Type	Corporate Credit or Debit Card Numbers
Department name and/or number	End Date
EPO access badge number	Hours of Work

Job Title Role	Language preference (of communication)
Office Location	Previous Work History
Unknown	
EPO badge validity	Price list for discounts
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name
Gender	Surname
Nationality	Picture
Signature	
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
Network/application Interaction Data	
Session details	
Health Data	
Health Data	
Contact Information	
Contact Details	Emergency Contact Details
Home Address	Personal Email
Phone Numbers	Working email address
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
IDP	Instructor related data
Learning external events	Learning history
Learning plan	Ratings

Social learning inputs	
Professional Experience & Affiliations	
CV	Political Affiliation and Activities
Professional Memberships	Qualifications Certifications
European Patent Register Data	
Address	Data provided by the data subjects
Correspondence	
Personal information provided voluntarily	
Patent Process Related Data	
Personal data potentially included within the content of a patent (claims, description, drawings, abstract)	
Financial	
Bank Account Information	Bank Account Number
Credit Card Number	Debit Card Number
Fund Reservation Requests	Information on home loans
Insurance Information	
Browsing Information	
Browsing Time	Cookie Information
IP Address	Network Interaction History
Website History	
User Account Information	
Account Age	Account Number
Account Password	
Government Identifiers	
National Identity Card Details	Passport Number

Former Employees

Applications' Log	
SAP Logs	

Social	
Social Media Account	Social Media Contact
Social Media History	
Sensory and Electronic Information	
Audio Information	Electronic Information
Thermal Information	Time stamps from their access to the buildings
Visual Information	
Building area and site	
Building area and site	
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name
Gender	Height
Surname	Marital Status
Nationality	Picture
Racial or Ethnic Origin	Religion/Religious Beliefs
Sexual Orientation	Signature
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
Workplace Welfare	
Records of Personal Properties	
Contact Information	

Contact Details	Emergency Contact Details
Home Address	Home Leave Address
Personal Email	Phone Numbers
Previous Residence Address	Teleworking address
Working email address	
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
IDP	Instructor related data
Learning external events	Learning history
Learning plan	Social learning inputs
Correspondence	
Personal information provided voluntarily	
Health Insurance Information	
Insurance Policy Information	Unique Identifier for Subscriber
Ticketing	
Ticket related data	
Biometric	
Body temperature	Facial Recognition
Fingerprint	Voice Recognition
Background Checks	
Criminal History	Criminal Records
Drug Test Results	Reference or Background Checks
Employment Information	
Appeals Records Information	Benefits and Entitlements Data
Business Unit Division	Company Entity
Contract Type	Corporate Credit or Debit Card Numbers
Department name and/or number	Disciplinary Action

End Date	End Date and Reason for Termination
EPO access badge number	Exit Interview and Comments
Grade	Grievances and Complaints
Hours of Work	Job Application Details
Job Title Role	Language preference (of communication)
Line Reporting Manager	Military Status
Office Location	Performance Rating
Personnel Number	Previous Work History
Record of Absence/Time Tracking/Annual Leave	Salary
Start Date	Weight
Unknown	
EPO badge validity	Price list for discounts
Geolocation	
Geolocation Information	
Network/application Interaction Data	
Session details	
Health Data	
Health Data	
Professional Experience & Affiliations	
CV	Political Affiliation and Activities
Professional Memberships	Qualifications Certifications
Trade Union Membership	
Family Information	
Children's Names	Parents' Names
Spouse's information	Spouse's name
Financial	
Bank Account Information	Bank Account Number

Bank Statements	Bonus Payments
Compensation Data	Credit Card Number
Credit History	Debit Card Number
Fund Reservation Requests	Information on home loans
Insurance Information	Routing Number
Browsing Information	
Browsing Time	Cookie Information
IP Address	Network Interaction History
Website History	
User Account Information	
Account Age	Account Number
Account Password	Password
User ID	
Government Identifiers	
Driving Licence Number	National Identification Number
National Identity Card Details	Passport Number
Social Security Number	

Prospective Employees

Applications' Log	
SAP Logs	
Social	
Social Media Account	Social Media Contact
Ticketing	
Ticket related data	
Sensory and Electronic Information	
Time stamps from their access to the buildings	
Building area and site	

Building area and site	
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Background Checks	
Criminal History	Criminal Records
Drug Test Results	Reference or Background Checks
Employment Information	
Benefits and Entitlements Data	Business Unit Division
Company Entity	Contract Type
Department name and/or number	End Date
End Date and Reason for Termination	EPO access badge number
Grade	Job Application Details
Job Title Role	Language preference (of communication)
Line Reporting Manager	Military Status
Office Location	Performance Rating
Previous Work History	Salary
Start Date	Weight
Unknown	
EPO badge validity	Price list for discounts
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name
Gender	Height
Surname	Marital Status
Nationality	Picture

Religion/Religious Beliefs	Signature
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
Network/application Interaction Data	
Session details	
Health Data	
Health Data	
Contact Information	
Contact Details	Emergency Contact Details
Home Address	Personal Email
Phone Numbers	Working email address
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
IDP	Instructor related data
Learning external events	Learning history
Learning plan	Social learning inputs
Professional Experience & Affiliations	
CV	Political Affiliation and Activities
Professional Memberships	Qualifications Certifications
Correspondence	
Personal information provided voluntarily	
Financial	
Fund Reservation Requests	Information on home loans
User Account Information	
Account Age	Account Number
Account Password	Password
Government Identifiers	

National Identity Card Details	Passport Number

Recipient of the personal data

Recipients of the data Staff from D463 and PlanBit

Purpose of sharing Management of the contract (notification of equipment for collection, reporting on devices erased / deleted / recycled / reused).

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures Technical and organisational measures of PlanBit are described in the DPA. PlanBit is certified ISO27001 (and ISO 9001 + ISO 14001). Standard procedure for data removal is NIST-800-88 Purge, EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 184

Name Applications and patents related Legal advice

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 45 - CTO / BIT, DG4 - 46 - CIO / BIT

Entity Name - Controller (Entities) DG5 - 53 - Patent Law and Procedures

External processors

ServiceNow

External processors	
Name ServiceNow	

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

Global Lingo

External processors	
Name Global Lingo	

Requester

External processors

Name
Requester

OpenText

External processors
Name
OpenText

Microsoft

External processors
Name
Microsoft

OpenText

External processors
Name
OpenText

Atlassian/JIRA tool

External processors
Name
Atlassian/JIRA tool

TRE Thomson Reuters

External processors
Name
TRE Thomson Reuters

Microsoft

External processors
Name
Microsoft

ServiceNow

External processors
Name
ServiceNow

External processors	
Name Global Lingo	

Description of the processing

Description Upon request from EPO staff and, in selected case, from externals, D 5.2.1. provides legal and procedural advice in the form of explanatory notes, legal opinions or internal notes to specific applications or patents, drafts for legal texts, presentations, letters, speaking notes etc. (hereinafter “legal advice”). It includes replies to external enquiries not related to specific applications/patents, forwarded to D521 by EPO Customer Support via their tool (CSM/ServiceNow).

Personal data processed in this operation, if any, is provided by the requester.

All requests are registered in the case management system (Mattersphere or JIRA) under a specific Log number together with the requester’s and responsible officer’s names and assigned to the case handler within the Directorate.

Once the request has been assigned to the case handler the legal question is identified, assessed, and answered to the requester.

Receipt of the request, its processing and the provision of the reply may occur via e-mail, via chat functions or by any other tool available for intra-Office communication collaboration. The correspondence, drafts and final legal advice are saved in the CMS.

It might be necessary, during the elaboration of the advice, to consult other units of the Office, which might require the sharing of relevant personal data with them by email, by giving access to the document on a shared drive or by any other suitable means. This might also result in the further processing of personal data of staff members involved. In certain cases, such as publication in the official journal, amendment of EPC regulations, the tool OpenText/Common log is used for internal communication.

In the course of the above mentioned activities, it is also regularly necessary to record witness hearings during oral proceedings of the legal division involving D 5.2.1 is a member,

The active handling of a case stops when the entry in the CMS is closed in accordance with the applicable internal procedures.

This record covers also related organisational measures within the delegated controller's unit e.g. internal meetings, minutes' taking.

The personal data is kept until the end of the applicable retention periods.

Data Retention Personal data for non patent-file related matters is kept for the default retention time period for legal advice of Legal Affairs (20 years) except for cases where e. g. President, Vice President or other high ranked Officers were involved in order to be able to document the decision-making process.

Personal data in patent-file related matters (European patent applications and European patents) should be kept for thirty years to cover the longest possible period under Rule 147 EPC.

Purpose of Processing 1. The processing of personal data is necessary for providing legal advice on matters within the responsibility of Legal Affairs/D 5.2.1, mainly providing legal and procedural advice in patent law related matters, providing up-to-date information to stakeholders as well as all associated actions to e. g. ensure a proper and efficient information flow and management of associated activities., 4. Ensuring proper collaboration, consultation, alignment and hierarchy’s approval, 3. Deliver required advice, ensure proper preparation of subsequent actions (e.g. further communications, oral proceedings, final decision),, 5. preparation of statistics and overview for reporting purposes, 6. retrieval of previous advice as precedence, example and reference when dealing with new requests, with a view to harmonise internal and external practice., This encompasses: 2. Registering incoming requests,

Data subjects and categories of personal data

Employees

General	
Input provided during the deliberation and decision-making process	Legal opinions and assessments
Matter/Log file	
Attachments	Metadata
Ticketing	
Ticket related data	
Contact Information	
Contact Details	
Correspondence	
Additional Information which might be provided in the course of exchanges	
Employment Information	
Business Unit Division	Department name and/or number
Job Title Role	Office Location
Personal Identification	
Full Name	Gender

Externals

Matter/Log file	
Attachments	Metadata
General	
Any other information	
Ticketing	
Ticket related data	
Contact Information	
Contact Details	
European Patent Register Data	
Address	Data provided by the data subjects
Representation in EPO's Patent Granting Process	

Role in the Patent Grant Procedure	
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Personal information provided voluntarily	
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of a patent (claims, description, drawings, abstract)
Personal data potentially included within the content of patent procedure related information and publications	
Employment Information	
Company Entity	
Personal Identification	
Digital signature	Full Name
Gender	Signature

Recipient of the personal data

Recipients of the data 1) Requester
2) EPO hierarchy (above the delegated controller)
3) other units

Purpose of sharing 1) Requester (internal or external), who contacted legal affairs in the first place to obtain e.g. an advice
2) Hierarchy (when applicable) when the circumstances of a case require their information and/or decision.
3) other units (in some cases, colleagues from other units in the Office might need to be involved, on a need-to-know basis), as necessary to address a particular matter.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation 1) National Patent Offices
2) International Organisations such as WIPO
3) European institution such as EUIPO, CVPO

Transfer mechanism(s) The recipient provided appropriate safeguards, Legally binding and enforceable instrument between public authorities or bodies, Derogation in accordance with Art. 10 DPR

Country where data might be transferred - Processor (Vendors) Microsoft - United States, ServiceNow - Netherlands, TRE Thomson Reuters - Luxembourg, OpenText - United Kingdom, Global Lingo - United Kingdom

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, International cooperation activities, Public Authorities/Government Bodies

Derogations Art. 10 DPR The transfer is necessary for the performance of a task in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning, or to perform obligations arising from its duty of co-operation with the contracting states

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 205

Name Splunk

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG4 - 46 - CIO / BIT

External processors

Umbrio

External processors	
Name Umbrio	

Description of the processing

Description Splunk is a central log repository for security incident management enabling systems' protection by helping identify and analyse security issues.
The processing comprises (a) receiving technical data generated and already available from other BIT systems and services (b) performing automated queries for generating alerts for relevant security events (c) performing automated queries for generating dashboards and overviews of security relevant information
(d) performing manual queries for deeper analysis of security events, adaptation of dashboards and alerts.

Splunk receives technical data generated on (and available on) a number of EPO systems and services, in particular:
a. EPO-managed workstations assigned to EPO users
b. EPO-managed Servers
c. EPO-managed network equipment (e.g. routers, switches, firewalls, proxy servers)
d. External cloud providers with an established contractual relationship with the EPO (e.g. Microsoft, Google, Amazon, SAP)

Purpose of Processing Personal data is processed for the purposes of being able to identify the persons that carried out the activities that have been logged, in order to address any possible error or security incident that is detected. This is important because: • Log files are used to trace events in an information system and to help debugging and repair. They are part of the systems and are essential tools to provide the security and an efficient support when information systems are not working correctly. • Log files of EPO systems are processed for investigation and elimination of security incidents and malware infections on devices connected to the EPO network, and/or for prevention of data leaks. • Additionally, log files might be processed for statistical purposes or eliminating problems with users' access to EPO telecommunications systems. Any request for analysis of Splunk data other than to ensure the security and stability of EPO systems requires a separate, specific consultation with the DPO.

Data Retention Data which is stored on servers in Luxemburg is subject to the regular backup and archiving retention policy for on-premise servers.
Splunk log files are stored automatically and are kept for an agreed period of time depending on the type of information and the system to which it refers. Microsoft Defender for Endpoint Security alert/incident related data is retained for 12 months within Splunk. Data is kept in Splunk for up to 18 months, after which it is automatically deleted. Data is kept in backups for 60 days after expiration from Splunk system, after which it is no longer available.
As a result, Splunk's overall data retention never exceeds 20 months.

Data subjects and categories of personal data

Contractors

Phone Call Information	
Called Phone Number	Caller's Phone Number
Phone Call Date and/or Time	Phone Call Duration
Phone Call Interaction History	
Network/application Interaction Data	
Session metadata	
Ticketing	
Ticket related data	
Physical and/or Digital Identifiable Assets	
Operating System Version	Workstation Serial Number
Workstation's Hostname (Physical or Virtual)	Workstation's Network Adapter MAC address
Contact Information	
Phone Numbers	Working email address
Telephony Interaction Data	
Telephony Session Metadata	
Browsing Information	
Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
Category	IP Address
Network Interaction History	URL
Website History	

Employment Information	
Active/Inactive Indicator	Contract Type
Department name and/or number	End Date
Job Title Role	Language preference (of communication)
Line Reporting Manager	Office Location
Personnel Number	Room Number
Start Date	
Personal Identification	
First Name	Full Name
Gender	Surname
Geolocation	
Geolocation Information	
User Account Information	
Account Number	User ID
System Logs	
Audit Logs (a.k.a. Audit Trail)	File data (name, size and/or hash)
Firewall/Router/Switch Logs	Ports
Registry data	Running Processes
System-, Application-, Security-related Server Logs	Transaction-related Details
Web Servers Logs	

Employees

Phone Call Information	
Called Phone Number	Caller's Phone Number
Phone Call Date and/or Time	Phone Call Duration
Phone Call Interaction History	
Network/application Interaction Data	
Session metadata	
Ticketing	

Ticket related data	
Physical and/or Digital Identifiable Assets	
Operating System Version	Workstation Serial Number
Workstation's Hostname (Physical or Virtual)	Workstation's Network Adapter MAC address
Contact Information	
Mobile Phone Number	Phone Numbers
Working email address	
Telephony Interaction Data	
Telephony Session Metadata	
Browsing Information	
Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
Category	IP Address
Network Interaction History	URL
Website History	
Employment Information	
Active/Inactive Indicator	Contract Type
Department name and/or number	End Date
Job Group	Job Title Role
Language preference (of communication)	Line Reporting Manager
Office Location	Personnel Number
Room Number	Start Date
Personal Identification	
First Name	Full Name
Gender	Surname
Geolocation	
Geolocation Information	
User Account Information	

Account Number	User ID
System Logs	
Audit Logs (a.k.a. Audit Trail)	File data (name, size and/or hash)
Firewall/Router/Switch Logs	Ports
Registry data	Running Processes
System-, Application-, Security-related Server Logs	Transaction-related Details
Web Servers Logs	

Externals

Phone Call Information	
Called Phone Number	Caller's Phone Number
Phone Call Date and/or Time	Phone Call Duration
Phone Call Interaction History	
Network/application Interaction Data	
Session metadata	
Ticketing	
Ticket related data	
Physical and/or Digital Identifiable Assets	
Operating System Version	Workstation's Hostname (Physical or Virtual)
Workstation's Network Adapter MAC address	
Telephony Interaction Data	
Telephony Session Metadata	
Browsing Information	
Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
Category	IP Address
Network Interaction History	URL
Website History	

System Logs	
Firewall/Router/Switch Logs	System-, Application-, Security-related Server Logs
Web Servers Logs	

Recipient of the personal data

Recipients of the data The only users of Splunk within PD 46 are BIT Information Security department and BIT Network and Data Centre Management department. All use of Splunk is to support security and network use cases, in abidance with need-to-know principle.
If other recipients request access to the personal data, this will be individually asked to the Delegated Controller consulting DPO for advice.

Purpose of sharing The purpose of sharing Splunk personal data to BIT Information Security and BIT Network and Data Center Management recipients is to cover the requirements of EPO's IT security and network use cases.
Any personal data can be processed as part of preventative, reactive and explorative use cases in compliance to the need-to-know principle, in so far as this is required to allow BIT support services to identify and locate the relevant systems and/or users. Explorative use cases are intended only for the purposes of identifying and fine-tuning new preventative or reactive use cases.

Any eventual request to analyse Splunk data having a purpose other than ensuring EPO systems' security and stability would require the preliminary, specific and separate consultation with the DPO.

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures Access Control - All queries using Splunk are done by authenticated users. Authentication is based on the EPO Active Directory systems, thereby ensuring that the normal account lifecycle management (such as deactivation of accounts for staff no longer in service) is implemented. -Access to Splunk is role-based. Active Directory groups govern which role/s a user belongs to, and roles are restricted in the type of information they can see in Splunk. -Only members of BIT Information Security and Network and Data Center Management departments can query data indexes containing personal data. Audit Trail -Splunk maintains a full audit trail of user queries and other activity. -The information, like any other information in Splunk, is "append only" so once written it cannot be altered or removed undetectably., EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 211

Name Booking process for office space and/or electrical charging station - SmartWay2 system - PD 4.4 General Administration

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 44 - General Administration, DG4 - 46 - CIO / BIT, DG4 - 4 - Corporate Services

Entity Name - Controller (Entities) DG4 - 44 - General Administration

External processors

Poornam

External processors	
Name Poornam	

Smartway 2

External processors	
Name Smartway 2	

Zendesk

External processors	
Name Zendesk	

Description of the processing

Description The tools will be use by all registered users to book office, rooms, or other facilities.

1. Procedure steps:

• The internal and external EPO users with an EPO email address in Azure Active Directory are automatically and daily uploaded into the Smartway2 booking system and get an smartway2 account created.
• Additional accounts for external users can be created manually by the administrator.
• The information stored will contain at least the first and last name of the person, its email address and possibly other information such as the organisation or the phone number. This information will be used to log into the system and will be used to identify users in the tool.
• Users are then allocated either manually or in a (semi-) automated way to groups depending on the access rights they should have.
• The user can decide to complement manually his/her profile with additional information such as his phone number.
• The user when performing/modifying a booking will enter the booking information (e.g. title, day, time, duration, room, invitees, services required, and any extra information) into the Smartway2 system directly or indirectly via Outlook. Invitees have to be users or contacts.
• Users can create contacts requiring at least display name and an email address and add the organisation and a phone number if they wish.
• A contact is created automatically in Smartway2 when the Smartway2 outlook plug-in is used to create booking and the Outlook invitation contains an invitee that does not already exist in Smartway2 as user or contact.The information stored is the email address and display name.
• Smartway2 system will store or update the booking. It will further create/modify the booking in the Outlook calendar of the user or send a corresponding Outlook invitation.
• Any user can see the bookings made for a specific room with the title of the booking, the host and the attendees list .
• If the booking is made private, the users only see a booked timeslot. Other information such as the title, host and attendees are not visible.
• Booking information is made accessible to Archibus to synchronise room occupancy, enable the triggering of services (e.g. catering, cleaning) and the generation of room usage reports.
• Users can search for the bookings and locations of a person as attendee or host unless the user has chosen not to allow the Find my colleague function.
• Information of current and previous bookings may be used for proposing the most suitable resource based on information such as the host or participants typical or current location (if using the app), the number of invitees, the title of the reservation.

2. New functionality: SW2 in Planning Tool and in Booking Statistics Dashboard.
A dahsboard functionality as been added to the booking tool:
• The Planning Tool provides to each staff member a view of the workplaces booked by his team members. In addition, users may grant access to any colleague to their Planning Tool information including their workplace bookings. In such case the colleague can access this information using the Custom teams feature of the Planning Tool.
• The Planning tool does not store any booking information. It retrieves the information from Smartway2 at the time the user loads or refresh the Planning Tool page.
• The Room booking statistics dashboard is updated daily at 8:00 with the booking information extracted at 2:00. Beside anonymous room booking statistics, the manager can see the workplace bookings of all the staff in his unit and sub-units for the current and next 10 days.

3. Geo localisation services
• If allowed by the user and the mobile app activated, the location of be used to check the distance to a room to allow or forbid to check-in to the room. It could also be used to propose rooms in its vicinity.

4. NFC and iBeacon services
• The app provides a scan function enabling to scan a close by room panels to book or check-in/out as yourself.

Purpose of Processing Personal data is processed for the purpose of enabling users to book resources (e.g. rooms, desks, charging stations) and/or invite colleagues to a meeting, and manage the utilisation of resources. The processing of personal data is necessary for: - Automatically adding users to the directory of the booking system - Creating and managing bookings - Accessing and viewing own bookings - Inviting attendees - Managing access rights - Notifying users for reminder - Creating usage report - Checking-in/out of a room, desk… - Helping colleagues to find each other colleagues by allowing users to authorise if they wish colleagues to search their room bookings as host or attendee - Generating anonymous reports on room occupancy and usage - Create/modify bookings in outlook

The app requires permission for Geo localisation, NFC and iBeacon to work at its . If this services are turned off at the device level, the app still works without these extra featuress

Data Retention Booking information is stored for a maximum of 6 years after the booked day

Data subjects and categories of personal data

Contractors

Contact Information	
Working email address	
Personal Identification	
Full Name	

Employees

Contact Information	
Working email address	
Personal Identification	
Full Name	
Geolocation	
Geolocation Information	

Externals

Contact Information	
Working email address	
Personal Identification	
Full Name	

Recipient of the personal data

Recipients of the data Personal data registered in the booking system are accessible to 442 team working in Space management, service line during the retention period established and for the performance of their duties (monitoring and managing space occupancy).

BIT - PD 46 - for IT activities which might require access to the personal data contained in this process

Purpose of sharing

Transfer

Transfer No

Country where data might be transferred - Processor (Vendors)
Smartway 2 - India, Smartway 2 - United States

Transfer to public authority and/or International Organisation	**Reasons for the transfer** Service provider processing data only for Operations/Maintenance purposes
Transfer mechanism(s) The recipient provided appropriate safeguards	**Derogations Art. 10 DPR**

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: - physical security measures; - access control measures: role-based, principles of need-to-know and least privilege; - storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers; - user control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, antimalware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; - transmission control measures: audit logging, System and network monitoring; - input control measures: audit logging, System monitoring; conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 212

Name Contact Center Solution - Anywhere 365

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG4 - 46 - CIO / BIT

External processors

Workstreampeople B.V.

External processors	
Name Workstreampeople B.V.	

Intrasoft International S.A.

External processors	
Name Intrasoft International S.A.	

Indra Soluciones Tecnologias de la Información, S.L.U.

External processors	
Name Indra Soluciones Tecnologias de la Información, S.L.U.	

Infeurope S.A.

External processors	
Name Infeurope S.A.	

Microsoft

External processors	
Name	
Microsoft	

Description of the processing

Description The EPO's Contact Center Solution - based on Anywhere 365 - is the platform leveraged by various contact centers of the EPO to manage incoming phone calls, to route them to the correct call center agent, to use interactive voice response (IVR) and call queue functionalities, to manage and distribute call volumes, to log phone calls' metadata and move them into a cloud-based business analytics environment (Microsoft PowerBI) . Calls metadata loaded onto Power BI enable each defined contact center to derive reports on own portion of calls metadata.
Only the EPO call centers which have explicitly requested to Delegated Controller to be enabled to use the call-recording feature are technically allowed to do so; storage location and retention of recorded audio files are decided and enforced by the given call center's Delegated Controller.
By default Anywhere 365's recorded audio files get stored in EPO's Microsoft 365 cloud.

Data Retention -Anywhere Dialogue Cloud conferencing backend log files: retained in Azure Log Analytics Workspace for 30 days; retained on disk for 2 days for backup purposes. Overall retention: 32 days.

-Call Data Records (CDR): for any given EPO call centre, the CDR retention time is decided by its corresponding Delegated Controller; currently the CDR of any call centre is retained for 365 days in a Microsoft Azure SQL Database within EPO's Azure tenant.

-Audio recordings: audio recording of phone calls is currently configured only for BIT Service Desk call centre. Audio files are stored in Sharepoint Online Library in EPO's tenant for one month.

-Reports by PowerBI are kept according to retention rules decided by the specific Delegated Controller that is accountable for the given Call Centre.

Purpose of Processing Purposes of the present processing operation are: enabling and provision of call center services to various EPO stakeholders on top of basic telephony; configuration, operation and maintenance for each logically defined call centre; acceptance and routing of incoming phone calls to the correct EPO agent, also by means of IVR and call queue functionality; management of call recording and storage of recorded audio files (such option is implemented only for specific call centres); logging of call activities to manage, monitor, troubleshoot, derive statistical reports and deliver a state-of-the-art service.

Data subjects and categories of personal data

Contractors

Phone Call Information	
Called Phone Number	Caller's Phone Number
Phone Call Date and/or Time	Phone Call Duration
Phone Call Interaction History	Phone Calling History
Network/application Interaction Data	
Session details	Session metadata
Sensory and Electronic Information	
Audio Information	Presence Status

Contact Information	
Phone Numbers	Working email address
Telephony Interaction Data	
Recorded Audio File	Telephony Session Content
Telephony Session Details	Telephony Session Metadata
Personal Identification	
First Name	Surname
User Account Information	
Account Number	Application Specific User Role
Membership Permissions	Ownership Permissions
User ID	
System Logs	
Audit Logs (a.k.a. Audit Trail)	System-, Application-, Security-related Server Logs

Employees

Phone Call Information	
Called Phone Number	Caller's Phone Number
Phone Call Date and/or Time	Phone Call Duration
Phone Call Interaction History	Phone Calling History
Network/application Interaction Data	
Session details	Session metadata
Sensory and Electronic Information	
Audio Information	Presence Status
Contact Information	
Phone Numbers	Working email address
Telephony Interaction Data	
Recorded Audio File	Telephony Session Content
Telephony Session Details	Telephony Session Metadata
Personal Identification	

First Name	Surname
User Account Information	
Account Number	Application Specific User Role
Membership Permissions	Ownership Permissions
User ID	
System Logs	
Audit Logs (a.k.a. Audit Trail)	System-, Application-, Security-related Server Logs

Externals

Phone Call Information	
Called Phone Number	Caller's Phone Number
Phone Call Date and/or Time	Phone Call Duration
Phone Call Interaction History	Phone Calling History
Sensory and Electronic Information	
Audio Information	
Contact Information	
Contact Details	Country
Home Address	Mobile Phone Number
Personal Email	Phone Numbers
Private Phone Number	Working email address
Telephony Interaction Data	
Recorded Audio File	Telephony Session Content
Telephony Session Details	Telephony Session Metadata
Personal Identification	
First Name	Surname

Recipient of the personal data

Recipients of the data The EPO-internal person responsible for a given Contact Centre and his/her deputies have access to only the data for their own contact centre.

Recipients of personal data are:
- supplier's staff who operates and maintains Anywhere 365 SaaS cloud solution;
- Anywhere 365 overall administrators within EPO 4.6.1.5;
- EPO contractors and employees working as call center agents or call center responsible (for a given Contact Centre defined in Anywhere 365);
- EPO call center responsible people and/or their deputies, who access own call center's reports via PowerBI;
- (only in case of call recording) BIT staff responsible for the administration of the EPO Sharepoint Online where audio recordings are stored.

Purpose of sharing Personal data are shared:
- to the Anywhere 365 staff (SaaS supplier): for operation and maintenance and service delivery of the SaaS solution

- to staff in BIT 4.6.1.5: to configure and perform the overall IT administration of EPO's Anywhere 365 instance and of the various call centres defined therein; to manage the recorded calls' audio files saved in Sharepoint Online (only if recording is enabled for the given call centre); to manage, monitor, troubleshoot, and keep the Call Centre service at state-of-the-art; to run statistical reports in PowerBI for the benefit of the given Call Centre.

- to EPO contractors and employees working as Call Centre agents or Call Centre responsible: to deliver and manage the specific Call Centre service.

- to EPO employee responsible for a given Call Centre: to access aggregated reports specific for own Call Centre.

Transfer

Transfer No

Country where data might be transferred - Processor (Vendors) Microsoft - United States

Transfer to public authority and/or International Organisation

Reasons for the transfer

Transfer mechanism(s)

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures WorkStreamPeople B.V. Anywhere365 is ISO27001 and NEN7510 certified., EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 215

Name Videoconferencing via Zoom

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG4 - 46 - CIO / BIT

External processors

Zoom

External processors	
Name Zoom	

Zoom

External processors	
Name Zoom	

Description of the processing

Description Zoom Video Communications ("Zoom") is a cloud-based videoconferencing (VICO) platform enabling the - successful - organisation of events in a virtual environment such that effective interaction between participants is as close as possible to a face-to-face experience.

With a view to the needs of the Office and its stakeholders to continue enjoying access to all services the EPO has extended the use of videoconference in order to organise virtual events. Within this framework, Zoom is used for conducting such virtual events, in particular for events where simultaneous interpretation is required, such as for example oral proceedings or board meetings with Member States (AC, BFC, etc.)

Personal data is processed in the Zoom platform for the purpose of carrying out the virtual event and ensuring the effective collaboration and communication between the Office and its stakeholders thus guaranteeing EPO business operations and compliance with applicable legal obligations. The collected data may also be used to prepare anonymised statistics on the meetings and participants such as type of meeting, number of meetings, average duration, meeting interruptions and reconnections, etc. for quality and volume monitoring purposes.

In addition, Zoom may process some personal data for its own Legitimate Business Purposes, as an independent Controller, solely when the processing is strictly necessary and proportionate and for one of the following purposes: a) directly identifiable data for the purposes of - billing, account and customer relationship management and relating correspondence - complying with and resolving legal obligations - abuse detection, prevention and protection, virus scanning and scanning to detect violations of terms of service and b) pseudonymised and/or aggregated data for - improving and optimising the performance and core functionalities - internal and financial reporting, revenue and capacity planning, forecast modelling - receiving and using feedback for overall service improvement.

Personal data eventually present in Zoom may be subject to additional processing operations done according to other purposes.

As part of the nature of a collaborative tool, additional personal data may be included in the information that is exchanged between meeting participants during a particular meeting or event, such as instant messages (chat), images, files, whiteboards, transcripts and recordings. Any such purposes are established by the organisational unit to which a specific user belongs to, represented by the Delegated Controller of the organisational unit.

Recordings via Zoom are done only if strictly necessary for legitimate and explicit purposes and approved in advance; default setting is that no one can record. The user is automatically notified when a recording starts and will be given the option to leave the virtual event in case he/she does not wish to be recorded.

Data Retention Zoom shall retain the personal data of the attendees strictly necessary for the organisation and management of a particular event/meeting for the maximum of one month.

Purpose of Processing Personal data is processed for the purpose of conducting videoconferences / virtual events organised by the EPO.

Data subjects and categories of personal data

Contractors

General	
Answers to surveys, assessments or quizzes	

Network/application Interaction Data	
Session metadata	
Physical and/or Digital Identifiable Assets	
Mobile Device Name	Mobile Device's Network Adapter MAC Adress
Operating System Version	Workstation's Hostname (Physical or Virtual)
Workstation's Network Adapter MAC address	
Contact Information	
Contact Details	Country
Phone Numbers	Working email address
Device Management Data	
Account ID	MAC Address
Platform-specific IDs	
Correspondence	
Additional Information which might be provided in the course of exchanges	Chat content
Personal information provided voluntarily	
Telephony Interaction Data	
Telephony Session Metadata	
Browsing Information	
Browser type	Browser User Agent
Cookie Information	IP Address
URL	
Geolocation	
Geolocation Information	

Employees

General	
Answers to surveys, assessments or quizzes	
Network/application Interaction Data	
Session metadata	

Physical and/or Digital Identifiable Assets	
Mobile Device Name	Mobile Device's Network Adapter MAC Adress
Operating System Version	Workstation's Hostname (Physical or Virtual)
Workstation's Network Adapter MAC address	
Contact Information	
Contact Details	Country
Phone Numbers	Working email address
Device Management Data	
Account ID	MAC Address
Platform-specific IDs	
Correspondence	
Additional Information which might be provided in the course of exchanges	Chat content
Personal information provided voluntarily	
Telephony Interaction Data	
Telephony Session Metadata	
Browsing Information	
Browser type	Browser User Agent
Cookie Information	IP Address
URL	
Geolocation	
Geolocation Information	

Externals

General	
Answers to surveys, assessments or quizzes	
Network/application Interaction Data	
Session metadata	
Physical and/or Digital Identifiable Assets	
Mobile Device Name	Mobile Device's Network Adapter MAC Adress

Operating System Version	Workstation's Hostname (Physical or Virtual)
Workstation's Network Adapter MAC address	
Contact Information	
Contact Details	Country
Phone Numbers	Working email address
Device Management Data	
Account ID	MAC Address
Platform-specific IDs	
Correspondence	
Additional Information which might be provided in the course of exchanges	Chat content
Personal information provided voluntarily	
Telephony Interaction Data	
Telephony Session Metadata	
Browsing Information	
Browser type	Browser User Agent
Cookie Information	IP Address
URL	

Former Employees

General	
Answers to surveys, assessments or quizzes	
Network/application Interaction Data	
Session metadata	
Physical and/or Digital Identifiable Assets	
Mobile Device Name	Mobile Device's Network Adapter MAC Adress
Operating System Version	Workstation's Hostname (Physical or Virtual)
Workstation's Network Adapter MAC address	
Contact Information	

Contact Details	Country
Phone Numbers	Working email address
Device Management Data	
Account ID	MAC Address
Platform-specific IDs	
Correspondence	
Additional Information which might be provided in the course of exchanges	Chat content
Personal information provided voluntarily	
Telephony Interaction Data	
Telephony Session Metadata	
Browsing Information	
Browser type	Browser User Agent
Cookie Information	IP Address
URL	
Geolocation	
Geolocation Information	

Recipient of the personal data

Recipients of the data - EPO Staff and external users
- Members of the department 4615 PACE
- Zoom

Purpose of sharing The personal data is disclosed, on a need to know basis, to the following recipients:

- the EPO's staff members and external users participating in or organising virtual events;
- Members of the department 4615 - PACE (Productivity Apps, Collaboration &Events)
- Zoom and its third-party providers for service maintenance and support purposes.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) Data Protection EU Comm Standard Contractual Clauses

Country where data might be transferred - Processor (Vendors) Zoom - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures	Zoom has SOC 2 type II certification for compliance with security, availability, processing, integrity and confidentiality standards and its cloud services provider is ISO 27001 certified., EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 217

Name EQE - European Qualifying Examination

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 46 - CIO / BIT, DG4 - 45 - CTO / BIT, DG4 - 41 - Finance

Entity Name - Controller (Entities) DG5 - 54 - Patent Intelligence

External processors

UNIwise

External processors	
Name UNIwise	

Comm100 Network Corporation

External processors	
Name Comm100 Network Corporation	

Maintenance company in charge of the service of the application (Portier)

External processors	
Name Maintenance company in charge of the service of the application (Portier)	

G.A.S.T

External processors

Name
G.A.S.T

Microsoft

External processors
Name
Microsoft

UNIwise

External processors
Name
UNIwise

Description of the processing

Description Personal data is processed by the EPO to successfully organise and manage the European Qualifying Examination and follow-up actions in accordance with Article 134 EPC and the Regulation on the European qualifying examination (REE) and its Implementing provisions (IPREE).

The present document aims at providing information on how the personal data are processed in the context of the different stages and activities of the EQE, such as the registration and enrolment of the candidates, the correct performance of the examination, the provision and publication of the result and the appeals as well as the selection and appointment of the Committees members.

The examination is organised and conducted by a Supervisory Board, an Examination Board, Examination Committees and an Examination Secretariat. The composition and duties of the bodies as well as the procedures to appoints their members are regulated in the REE (Articles 2 to 10) and IPREE. The names of the members are published online once they have been appointed by the President.

Members of the Supervisory Board, Examination Board and Examination Committees provide their data when applying to become member of the respective body. The information is entered into the system by the Examination Secretariat.

According to Rules 1 and 28 IPREE and Article 11 REE, candidates intending to enrol for the European qualifying examination (EQE) for the first time must register once they have commenced their professional activity within the meaning of Article 11(2) REE. Candidates must upload all supporting documents to the web portal: documentation that proves their identity, academic qualifications and professional requirements. When required, paper documents are entered into the systems by the Examination Secretariat.

Formal requirements are assessed by the Examination Secretariat, who decides on the registration and enrolment of candidates in accordance with the REE and the IPREE. The Examination Secretariat checks if the formal requirements are met and, in case of doubt, asks the provider of the data for further evidence.

These activities include the processing of personal data for the registration for the assessment of special cases (disabilities), for the candidates' enrolment as well as for the payment of the fees.

Purpose of Processing Personal data is processed by the EPO to successfully organise and manage the European Qualifying Examination and follow-up actions in accordance with Article 134 EPC and the Regulation on the European qualifying examination (REE) and its Implementing provisions (IPREE).

Candidates with disabilities are flagged in the system as needing special arrangement, the medical details of the disability as such are not named nor stored, since only compensation is offered. Correspondence with candidate is kept in his/her file as long as the candidate is active in the EQE.

The exam can be done via an online platform.

The external supplier that provides the online platform process personal data on the EPO's behalf and it is in charge of the maintenance of the platform and offering support. The online platform has proctoring features to monitor the candidates during the examination to prevent attempts of fraudulent behaviour and keep proof of them, where deemed necessary.

The answers are marked, and the results provided by the markers via the online portal and verified by the Examination Board. The results are made available by the Examination Secretariat to each candidate together with the marking sheets pertaining to his answer papers.

According to Article 21 REE, candidates' anonymity shall be respected when their answers are marked and their answers may be published for research, statistical or training purposes provided their anonymity is respected.

The appeal procedure before the Disciplinary Board of Appeal under Article 24 REE. follows the rules before said Board and the additional Rules of Procedure of the Disciplinary Board of Appeal of the European Patent Office.
The texts of these Rules, the business distribution schemes of the Boards and other information on the Boards and the appeals procedures are contained in the annual supplementary publication to the EPO Official Journal "Information from the Boards of Appeal".

Data is additionally processed for the purpose of surveying participants for feedback, including from EQE candidates, relating to the examination experience including specific issues related to disabilities and specific conditions. Anonymised statistical analysis information may be shared with third parties.

Data Retention Reasons are explained in the Annex: Archiving and Retention policy for the European qualifying examination (EQE) - decision by the Supervisory Board of the EQE

The retention periods for different types of documents are determined by consideration of the operational, legal and contractual requirements, and in line with best practice. The periods are counted from the final decision or latest action.

The length of retention is based on good practice, proof of final award (i.e. requirements of Art.134 EPC fulfilled), avoid fraudulent behaviour and financial accountability.

Data subjects and categories of personal data

Employees

General	
Any other information	
Contact Information	
Contact Details	Emergency Contact Details

Phone Numbers	Working email address
Building area and site	
Building area and site	
Professional Experience & Affiliations	
CV	Qualifications Certifications
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Employment Information	
Department name and/or number	Language preference (of communication)
Office Location	Personnel Number
Personal Identification	
Age	Date of Birth
Disability or Specific Condition	First Name
Full Name	Gender
Surname	Nationality
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
Government Identifiers	
Passport Number	

Externals

General	
Any other information	
Health Data	
Mobility needs	
Sensory and Electronic Information	
Audio Information	

Contact Information	
Contact Details	Phone Numbers
Working email address	
Biometric	
Facial Recognition	Voice Recognition
Professional Experience & Affiliations	
CV	Qualifications Certifications
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Online invigilation data	
Audio input	Webcam captures
Employment Information	
Company Entity	Department name and/or number
Job Title Role	Language preference (of communication)
Office Location	
Personal Identification	
Age	Date of Birth
Disability or Specific Condition	First Name
Full Name	Gender
Surname	Signature
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
Government Identifiers	
National Identity Card Details	Passport Number

Recipient of the personal data

Recipients of the data The Supervisory Board, the Examination Board, Examination Committees and an Examination Secretariat have access to the data of candidates to the extent needed to perform their respective duties as defined in the REE.

Depending on the EQE body, access to the data is granted on a need-to-know basis to EPO and non-EPO staff.

According to Article 23 REE: subject to Articles 21(2) and 22 REE, the members and deputy members of the Supervisory Board and the members of the Examination Board, the Examination Committees and the Secretariat shall be bound to secrecy both during and after their term of office with regard to all matters concerning the preparation of examination papers, the candidates and any relevant deliberations. The personal data is disclosed, on a need-to-know basis, to the following recipients:
• the EPO's staff members of the Examination Secretariat;
• members of the Examination Committees and the Examination Board;
• EPO authorised users (`master` users);
• Administrators of the WISEflow platform at UNIWise and its subprocessors (management of ticketing of incidents and to the following data of the candidates and the members of the Examination Committees for the bidirectional communication channel (chats) during the examination; hosting services);BIT
• Finance departments for the fee processing
• Disciplinary Board of Appeal

Purpose of sharing For the purpose of organising and conducting the examination.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) Data Protection EU Comm Standard Contractual Clauses

Country where data might be transferred - Processor (Vendors)
UNIwise - European Union, Microsoft - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, Service provider's sub-processor is based in a third country

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums)., To mitigate the risk of a conflict of interest within the EPO (EPO employees may sit the examination) access to data is restricted to a very limited group of persons. Technical means protect the violation of confidentiality as far as possible, even from system administrators. Technical staff of the service providers who cannot be exempted from access are individually known and bound by a confidentiality declaration. All personal data are stored in secure IT applications according to the security standards of the EPO. External providers are under strict contractual obligation as defined by Procurement and BIT standards. Limited access to data is given to technical staff of the provider on an event driven basis for the purpose of system administration and error analysis. For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. Except for a specific purpose defined in advance by the DPS, only the minimum necessary data are shared with other external parties. These parties have systems which are in conformity with the EPO security standards and have implemented the appropriate technical and organisational measures in this respect. All EQE members are bound by secrecy under Article 23 REE. Access to these data is protected by the personal user accounts of the EB members. Marking of the answers is anonymous. Financial procedures for the administration of fee payment are executed by the EPO Finance department and their service providers.

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 225

Name Staff requests that require medical assessments by the EPO Medical Services

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 41 - Finance, DG4 - 422 - People Engagement and Partnership, DG4 - 46 - CIO / BIT

Entity Name - Controller (Entities) DG4 - 423 - HR Essential Services

External processors

SAP

External processors	
Name SAP	

Microsoft

External processors	
Name Microsoft	

Cigna

External processors	
Name Cigna	

Microsoft

External processors

Name
Microsoft

Description of the processing

Description This record refers to the medical assessments carried out by the EPO Occupational Health Services (OHS) upon request of the staff and in the cases provided for by the Service Regulations.

The staff of the OHS consists of medical and administrative staff.

The medical staff provide medical assessments in the following cases:
a. Assessment of dependants' disabilities or serious illness for the granting of special allowances and reimbursement:

Staff members can request via a MyFIPS online form the assessment of the medical conditions of their dependants for the granting of the allowances under Article 69(5)(8) and the reimbursements under Article 69(10) ServRegs. The request is received by the OHS staff and is stored in the EPO medical database (Cority).

The conclusion of the medical assessment (that do not contain any medical information) is sent to the requester and HR Salary Department for registration of the relevant information in FIPS and for payment purposes.

If the request is sent via the HR ticketing system, the HR Interlocutors will also have access to the administrative information of the request, but not to any medical information.

Outlook may also be used for sharing information between the OHS and the requester. If the OHS have to share any confidential medical information with the requester, the file containing such information will be encrypted or password protected.

Relevant legal provisions: Article 69(5)(8)(10), Article 89-90 ServRegs

b. Assessment of family member's illness for the granting of special and family leaves

Staff members send their requests to the HR Interlocutors via the HR ticketing system and per email they send the required medical information to the OHS.

Any medical information is stored by the in the medical database.

The conclusion of the medical assessment (that do not contain any medical information) is sent to the HR Interlocutors via email for registration of the relevant information in FIPS. HR Interlocutors will also inform the requester and their line manager on the conclusions of the medical assessment (which does not contain any medical information).

Relevant legal provisions: Article 45b(1) ServRegs, Circ. 22 Rule 3 Article 45b(c)(ii)(iii) ServRegs, Article 59(3) ServRegs, Circ. 22 Rule 8 Article 59 ServRegs

c. Settlement of disputes between staff and the health insurance administrator (Cigna) on reimbursement of medical expenses
Staff members send their request normally via MyFIPS online form or email to the OHS. The medical information provided is stored in the medical database.

Exchange of information via email for the settlement of the disputes between Cigna and the OHS is possible and is encrypted via TSL (transport layer security). The conclusion of the medical assessment is sent to the requester and Cigna via email and, in principle, does not

contain medical information.

In some specific cases and in order to prevent any reimbursement disputes, Cigna may ask OHS for advice on the eligibility for reimbursement of a medical treatment. In these cases, the medical documents are, in principle, anonymized.

Relevant legal provisions: Circ. 236, Circ. 178, Article 89-90 ServRegs

c. Grant sick leave for spa cures

The request for a spa cure (A or B type) is sent by the staff member via MyFIPS online form to the OHS.

Family members and pensioners send requests for cures of type A per email to OHS. The request contains a medical prescription and report. The medical assessment of the OHS medical staff on the granting of the sick leaves is based on the said document.

The assessment is sent via email to the HR Interlocutors for the registration of the sick leaves in the HR database (SAP-FIPS), to the line manager and for cure of type A also to Cigna. This assessment does not contain any medical information.

The communication via email between Cigna and the OHS is encrypted via TSL (transport layer security).

Family members and pensioners send requests for cures of type B per email to Cigna directly.

Relevant legal provisions: Art 83 ServRegs , Circ. 367 Article. 1D Sick leave in case of spa cures, Circ. 368 Guide to Cover

In all the cases mentioned above:
•There is no exchange of medical information between the OHS staff and the management, the HRBP and the HR Interlocutors.
•Any medical information (e.g. date of the consultation, medical notes, medical reports) is stored in the EPO medical database (Cority)

Data subjects are:
•Employees
•Pensioners (for a. ,c., d. case)
•External (Employees' and pensioners' family members (for the d. cases), widow, heirs (for the a., c., d. cases), treating physicians of the requester)

In all the above-mentioned procedures, the following categories of personal data may be processed:

Surname, forename, gender, personnel number, date and place of birth, nationality, civil status, children's name and date of birth, languages, postal addresses, e-mail address, telephone numbers, room number, name, contact details of the treating physician, job profile, type of contract, line manager name, type and duration of absences from work, date/time of medical consultations, sickness statistics, sick leave certificates, medical opinions (always issued without medical data).

In all the above-mentioned procedures, the following special categories of personal data may be processed.

Medical data: personal medical history, medical reports provided by the staff member, medical reports provided by EPO specialists after a consultation with the employee, medical notes recorded after a consultation, medical certificates, diagnoses.

Purpose of Processing Processing of medical data is necessary to • process the staff request for the granting of the benefits or the settlement of disputes as provided for in the Service Regulations • improve the wellbeing of staff and their family

Data Retention Cority is used since 2006 as main medical database. As of 2016, data are stored only electronically in the EPO medical data base.

Currently, the data is kept in the electronic database permanently due to technical constraints.

However, by 2024 the following retention periods should be implemented:
a. Assessment of dependants' disabilities or serious illness for the granting of special allowances and reimbursement - 5 years as of the end date of the allowance.
b. Assessment of family member's illness for the granting of special and family leaves - 5 years as of the case closure date.
c. Settlement of disputes between staff and the health insurance administrator (Cigna) on reimbursement of medical expenses - 10 years as of the case closure date.
d. Grant sick leave for spa cures - 10 years as of the case closure date.

The retention periods apply unless a litigation is pending. In case of pending litigation, the retention period will be suspended until all means of redress have been exhausted or the decision has become final.

All data stored in the Outlook common boxes and calendars of the OHS older than 5 years is deleted.

Personal data stored in SAP-FIPS have currently no retention period.

SAP-MyFIPS is used by the employees to send requests for cure, which are encryption protected. The encrypted data is automatically deleted from the server after 90 days and from the PC of the administrative staff when they confirm that the data has been uploaded to Cority MAU or on closing the encryption application (MedXfer).

In principle all data are stored only electronically. However, there are still old medical paper files stored in secured locked rooms only accessible to authorised staff that should be deleted by 2024.

Data subjects and categories of personal data

Employees

General	
Personal Information in SAP	Special Categories of Data in SAP
Ticketing	
Ticket related data	
Health Data	
Health Data	
Contact Information	
Contact Details	Country
Emergency Contact Details	Home Address

Personal Email	Phone Numbers
Working email address	
Correspondence	
Personal information provided voluntarily	
Family Information	
Children's Names	Child's birthday
Spouse's name	
Financial	
Bank Account Information	
Employment Information	
Contract Type	End Date
Grade	Hours of Work
Job Group	Job Title Role
Language preference (of communication)	Personnel Number
Room Number	
Personal Identification	
Age	Date of Birth
Full Name	Marital Status

Externals

Health Data	
Health Data	
Contact Information	
Contact Details	Home Address
Phone Numbers	
Financial	
Bank Account Information	
Personal Identification	
Age	Date of Birth

Disability or Specific Condition	Full Name

Former Employees

Ticketing	
Ticket related data	
Health Data	
Health Data	
Contact Information	
Contact Details	Home Address
Personal Email	Phone Numbers
Family Information	
Children's Names	Spouse's name
Financial	
Bank Account Information	
Employment Information	
End Date	
Personal Identification	
Age	Date of Birth
Disability or Specific Condition	Full Name
Marital Status	

Recipient of the personal data

Recipients of the data The following recipients may have access to the categories of personal data (excluding medical data) mentioned under points 1.2 and 1.17 on a need-to-know basis only:

•HR Interlocutors – in particular they are the ones that may receive the request (in the a., b. cases) and process it once they receive the medical conclusion (in the b. cases)
•Line manager–is informed by the HR Interlocutors when the b. requests are granted and by the when d. requests are granted
•Legal Services may have access to personal data for the prevention and management of grievances
•Directorate Ethics and Compliance (DEC) may have access to personal data in the framework of their investigative mandate
•SAP–Centre of Excellence department – a very limited number of staff of this department provides technical support for the maintenance of the medical database (Cority), in particular for system configuration purposes (i.e. creation, update and deletion of general system settings including language; screen layouts including the configuration of fields displayed on screens; look-up tables; business rules including field input checks; roles and profiles) and users management (i.e. creation and deletion of user accounts and the assignment of roles)
•Microsoft Office
•SAP-FIPS

The following recipients may have access also to the medical data mentioned under point 1.2 and 1.17 on a need-to-know basis only:
•Treating physician of an employee – when the employee has expressly authorised the EPO medical staff to exchange information with their treating physician (according to Art. 89(3) ServRegs.
•Health insurance administrator (Cigna) – in the framework of processing cure requests, disputes on medical reimbursements, detecting health care frauds
•SAP–Centre of Excellence department – only one employee of this department with the role of system configurator is allowed to have full access also to medical data. This is a necessary requirement to ensure the functionality and efficiency of the application.

The data are not used for any other purposes nor disclosed to any other recipient.

Purpose of sharing

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors) Microsoft - United States, SAP - Germany, Cigna - United Kingdom, Cigna - Switzerland

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such

as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums)., The email exchange between the MAU and Cigna is secured via TLS (Transport Layer Security) which is intended to allow two email systems that normally communicate via SMTP (SMTP operates with no encryption) to establish a virtual encrypted “tunnel.” Once established, all of the communications between the two companies will pass through this tunnel, with the expectation that the information will be automatically encrypted., SAP-MyFIPS is used by the employees to send requests for cure, for special dependants’ allowances, settlements of medical reimbursement disputes which are encryption protected., Once a year (in Q1) a roles review and logs security audit is carried out. The user manager in SAP–Centre of Excellence department sends to the chief physicians of the EPO Health Services the list of users and their respective roles assigned to Cority. The chief physicians must verify and validate the list and roles. The logs security audit is done by the chief physicians directly, each one for the data they are responsible for., Administrative staff of the EPO Health Services, HR Interlocutors, HR Officers and the system configurator of the SAP-Centre of Excellence department are required to sign a confidentiality and data protection declaration, Medical reports are sent via email to the staff member after being encrypted or password protected in accordance with the Office’s recommendations (Outlook Migration to the Cloud-http://my.internal.epo.org/portal/private/epo/organisation/dg1/?WCM_GLOBAL_CONTEXT=/epo/intranet/organisation/dg1/vp1_org/announcements/2021/1612436889418_outlook_encripted_documents), When face-to-face consultations are not possible or the staff member prefers to have remote consultations, MS Teams is the application used in these cases. Staff is informed not to share messages or documents containing sensitive information during MS Teams (video)calls in accordance with the Office’s recommendations (Using Microsoft Cloud tools-http://my.internal.epo.org/portal/private/epo/work/news/?WCM_GLOBAL_CONTEXT=/epo/intranet/work/news/2020/1588753875455_using_cloud_based_tools)., The access to the medical data base is strictly given only to authorised persons, namely •the EPO medical and para-medical staff, •the administrative staff of the medical services, •the System Configurator of the SAP–Centre of Excellence department, •the Emergency User - In urgent cases it is essential that an emergency user exists, in order to intervene in cases of severe malfunction of the system (such as failure of the system, total authorisation blockage or process deadlock). Therefore the emergency user needs the complete Cority access rights. The emergency user has full authorisation allowing the execution of all system and application functions without any authorisation restrictions The access rights allow the above mentioned staff to process and consult only the data for which they are responsible

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 227

Name Identity Management through Okta

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG4 - 46 - CIO / BIT

External processors

Okta Inc

External processors	
Name Okta Inc	

Okta Inc

External processors	
Name Okta Inc	

Description of the processing

Description The EPO uses Okta's cloud-based software as a service (SaaS) platform for the purpose of Identity and Access management.

The processing operation involves user authentication via Okta. The authentication is required as soon as a user attempts to log in to a secure area of EPO online services that is accessible with a smart card or with account credentials obtained for using those customer facing services, such as for example Central Fee Payment, New User Area, Online Filing, eLearning, Bulk data download.

Okta is used for the coarse grained access, whereas the context based role definition and assignment is taken care of in the individual applications or services.

Purpose of Processing Identity and Access Management for externals

Data Retention - Logs are retained for 90 days
- Accounts can be deleted in Okta on request - or in any case will be deleted when the contract with Okta ends.
- Accounts associated with EPOLine credentials are retained in line with EPOLine data retention. If user (customer) is removed in EPOLine due to reaching the specified retention period or upon data subject request, then it will also be automatically removed in Okta.

Data subjects and categories of personal data

Externals

Network/application Interaction Data	
Session details	Session metadata
Physical and/or Digital Identifiable Assets	
Digital Certificate	Smart Card Number
Contact Information	
Mobile Phone Number	Personal Email
Working email address	
Employment Information	
Language preference (of communication)	
Browsing Information	
Browser type	IP Address
Network Interaction History	
Personal Identification	
First Name	Surname
User Account Information	
Account Number	Account Password

Employees

Network/application Interaction Data	
Session metadata	
Contact Information	
Working email address	
Personal Identification	
First Name	Surname

User Account Information	
Account Password	User ID

Recipient of the personal data

Recipients of the data Internal:
Information Security dept 4623
Staff in DG1
External:
Okta Inc and their affiliates

Purpose of sharing Internal:
Information Security dept 4623: for managing the identities and related access rights
External:
Okta Inc and their affiliates: to provide the identity and access management services (SAAS)

Transfer

Transfer Yes

Country where data might be transferred - Processor (Vendors) Okta Inc - Costa Rica, Okta Inc - United States

Transfer to public authority and/or International Organisation

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, To provide the identity and access management services

Transfer mechanism(s) The recipient provided appropriate safeguards

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums)., Okta maintains administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of our Data, including Personal Data, as set forth in the Trust & Compliance Documentation. Okta regularly monitors compliance with these safeguards, Okta has obtained certification under the Asia-Pacific Economic Cooperation scheme of Privacy Recognition for Processors and processes personal data accordingly.

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 229

Name Legal Affairs cooperation with CPVO - Joint Seminar

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG0 - 02 - Communication

Entity Name - Controller (Entities) DG5 - 53 - Patent Law and Procedures

External processors

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

Microsoft

External processors	
Name Microsoft	

Microsoft

External processors	
Name Microsoft	

Description of the processing

Description As part of the cooperation between the Office and the Community Plant Variety Office (CPVO), as agreed in an Administrative Arrangement between the EPO and CPVO, D521 organises and conducts bilateral virtual seminars involving representatives of both offices, in order to share knowledge and working practices on plant-related patents and plant variety rights.

For the purposes of organising these virtual seminars, personal data of the participants are processed.

Each meeting leads to opening of an electronic file in the case management system of the Directorate (CMS) under a specific Log number together with the name of the responsible officer to whom the organisation is assigned within the Directorate. Personal data are also processed in MS Outlook for correspondence purposes like sending invitations, distributing the agenda, etc.

In order to share knowledge and working practices on plant-related patents and plant variety rights.

A paper version of the file might also be printed.

The processing of the data will also serve possible follow-up actions after the meeting (like distribution of report).

Data Retention Personal data associated with the practical organisation of the EPO/CPVO seminar are kept as long as necessary for the organisation of seminars, usually yearly or at even longer intervals, in the context of the cooperation agreement. Contact details of participants indicated by CPVO for a given meeting are kept to facilitate the organisation of the next meeting until a person is no longer participating.

Personal data associated with the meeting file created in the case management system, including minutes and reports, are kept for he duration of the Administrative Arrangement and 20 years after that.

Purpose of Processing The CPVO seminars serve to implement the Administrative Arrangement and annual workplans with a view to streamlining international initiatives with impact on the Patent Grant Process ("PGP"), foster a holistic approach to IP training and awareness, further develop trust and collaboration between the two organisations.

Data subjects and categories of personal data

Employees

General	
Any other information	
Contact Information	
Phone Numbers	Working email address
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Personal information provided voluntarily	
Employment Information	
Job Title Role	
Personal Identification	

Full Name	Gender

Externals

General	
Any other information	
Contact Information	
Phone Numbers	Working email address
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Personal information provided voluntarily	
Employment Information	
Company Entity	Job Title Role
Personal Identification	
Full Name	Gender

Recipient of the personal data

Recipients of the data - CPVO
- PD02, EPO Event Management
- D521 Staff members
- D522 Staff members
- The external providers

Purpose of sharing Personal data is shared only with recipients who are involved in the logistics of organising the meeting.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation
Community Plant Variety Office (CPVO)

Transfer mechanism(s) The recipient provided appropriate safeguards, Derogation in accordance with Art. 10 DPR

Country where data might be transferred - Processor (Vendors)
Microsoft - United States, TRE Thomson Reuters - Luxembourg

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR The transfer is necessary for the performance of a task in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning, or to perform obligations arising from its duty of co-operation with the contracting states

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 230

Name Email usage

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG4 - 46 - CIO / BIT

External processors

Microsoft

External processors	
Name Microsoft	

Indra

External processors	
Name Indra	

Microsoft

External processors	
Name Microsoft	

Description of the processing

Description Processing of personal data occurs within the email and calendar flows from and to the mailboxes of EPO staff when using Microsoft Outlook and Exchange Online, as well as any service provider that has been assigned an EPO email address.

In addition Outlook also includes non-optional connected experiences which are designed to enable more effective creation, communication, and collaboration.

Purpose of Processing To enable the communication of e-mail messages, attachments and calendar-related actions amongst EPO staff and externals via user clients and Application Program Interfaces (APIs). -To offer to EPO email system users an address book to retrieve EPO recipients' addresses, mailing lists and groups -To have a trail of emails for IT troubleshooting and cybersecurity purposes. -To have a retention mechanism enabling EPO email system users to restore email messages which they have accidentally recently deleted. -Eventual requests to process Email usage personal data for purposes other than those stated above are to comply with Article 7 Circular 382 Information Security Guidelines.

Data Retention • Email information as well as any personal address book implemented by the EPO email system user is stored as long as the user wishes to maintain the message and as long as the user has a contractual obligation with the EPO.
• Email messages voluntarily deleted by the user are retained for 90 days and then purged.
• The personal information included in the Global address book and a user's mailbox is stored as long as a user (e.g. employee, contractor) has a contractual obligation with EPO. Once a contract expires, information is retained for maximum 1 year and a half for the purposes of collection from the EPO or possible renewal. After this period, information is deleted.
• In the cases of a legal claim or an administrative investigation, be it a disciplinary or criminal offense, personal data could be stored longer than the time limits indicated above. In such cases, which are out of BIT PD4.6 delegated controllership, the retention of personal data is decided on a case-by-case basis by the corresponding Delegated Controller.

At all times during the term of EPO's subscription, EPO will have the ability to access, extract and delete the data stored in Outlook and Exchange Online.
• Microsoft will retain EPO Data that remains stored in the Online Services in a limited function account for 90 days after expiration or termination of EPO's subscription so that Customer may extract the data.
After the 90-day retention period ends, Microsoft will disable EPO's account and delete the EPO Data and Personal Data stored in Online Services within an additional 90 days, unless authorised under the agreement with Microsoft to retain such data.
• For Personal Data in connection with the applications, Microsoft will delete all copies after the business purposes for which the data was collected or transferred have been fulfilled or earlier upon EPO's request, unless authorised under the agreement with EPO to retain such data.

Data subjects and categories of personal data

Contractors

Network/application Interaction Data	
Session content	Session details
Session metadata	
Sensory and Electronic Information	
Presence Status	
Physical and/or Digital Identifiable Assets	

Digital Certificate	Operating System Version
Workstation's Hostname (Physical or Virtual)	
Contact Information	
Contact Details	Phone Numbers
Working email address	
Correspondence	
Additional Information which might be provided in the course of exchanges	Personal information provided voluntarily
Employment Information	
Company Entity	Department name and/or number
Job Title Role	Office Location
Room Number	
Browsing Information	
Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
Cookie Information	IP Address
Network Interaction History	URL
Personal Identification	
Digital signature	First Name
Surname	
User Account Information	
Membership Permissions	Ownership Permissions
User ID	
System Logs	
Audit Logs (a.k.a. Audit Trail)	File data (name, size and/or hash)
System-, Application-, Security-related Server Logs	Transaction-related Details

Employees

Network/application Interaction Data

Session content	Session details
Session metadata	
Sensory and Electronic Information	
Presence Status	
Physical and/or Digital Identifiable Assets	
Digital Certificate	Operating System Version
Videoconference Room/Equipment Identifier	Workstation's Hostname (Physical or Virtual)
Contact Information	
Contact Details	Mobile Phone Number
Phone Numbers	Working email address
Correspondence	
Additional Information which might be provided in the course of exchanges	Personal information provided voluntarily
Employment Information	
Company Entity	Department name and/or number
Job Title Role	Line Reporting Manager
Office Location	Room Number
Browsing Information	
Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
Category	Cookie Information
IP Address	Network Interaction History
URL	
Personal Identification	
Digital signature	First Name
Surname	
User Account Information	
Membership Permissions	Ownership Permissions

User ID	
System Logs	
Audit Logs (a.k.a. Audit Trail)	File data (name, size and/or hash)
System-, Application-, Security-related Server Logs	Transaction-related Details

Externals

Network/application Interaction Data	
Session content	Session details
Session metadata	
Contact Information	
Personal Email	Working email address
Correspondence	
Additional Information which might be provided in the course of exchanges	Personal information provided voluntarily
Browsing Information	
Browsing Date and Time	IP Address
Network Interaction History	
Personal Identification	
Digital signature	First Name
Surname	
System Logs	
File data (name, size and/or hash)	System-, Application-, Security-related Server Logs
Transaction-related Details	

Former Employees

Network/application Interaction Data	
Session content	Session details
Session metadata	
Contact Information	
Contact Details	Mobile Phone Number

Personal Email	Phone Numbers
Correspondence	
Additional Information which might be provided in the course of exchanges	Personal information provided voluntarily
Browsing Information	
Browsing Date and Time	IP Address
Network Interaction History	
Personal Identification	
First Name	Surname
System Logs	
File data (name, size and/or hash)	System-, Application-, Security-related Server Logs
Transaction-related Details	

Prospective Employees

Network/application Interaction Data	
Session content	Session details
Session metadata	
Contact Information	
Contact Details	Country
Mobile Phone Number	Personal Email
Phone Numbers	Private Phone Number
Correspondence	
Additional Information which might be provided in the course of exchanges	Personal information provided voluntarily
Browsing Information	
Browsing Date and Time	IP Address
Network Interaction History	
Personal Identification	
First Name	Surname
System Logs	

File data (name, size and/or hash)	System-, Application-, Security-related Server Logs
Transaction-related Details	

Recipient of the personal data

Recipients of the data All EPO email system users.

BIT PD4.6 (Delegated Controller), more precisely BIT PACE 4615 and BIT Security 4623

The external processors.

Purpose of sharing All EPO email system users will have access to the Address Book information.

In the processing of email traffic and for the management of Exchange server, the only recipients are BIT PD4.6 (Delegated Controller) and the external processors which are tasked with the operation, maintenance and delivery of Exchange service.

More precisely, BIT PACE 4615 processes the personal data for email system administration, operation and maintenance purposes; while the recipients in BIT Security 4623 for email cybersecurity purposes.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors) Microsoft - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, Protection against malware, login to Azure Active Directory, error analysis, load balancing, diagnostics data, connected experiences, and processing for Microsoft's business operations

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures For personal data processed on systems not hosted on EPO premises, the providers processing the personal data have committed in a binding agreement to comply with their data protection obligations under the applicable data protection legal frameworks. The EPO has also carried out a privacy and security risk assessment. Any personal data in transit over public networks between the EPO and Microsoft, or between Microsoft data centres is encrypted by default. Personal data as part of any data that are provided to Microsoft by, or on behalf of, EPO through use of the Microsoft 365 services is encrypted at rest. Regarding the implementation of the encryption, Microsoft uses state of the art encryption technologies. Furthermore, Microsoft employs least privilege access mechanisms to control access to personal data which are part of data that are provided to Microsoft by EPO and role-based access controls are employed to ensure that access to such personal data required for service operations is for an appropriate purpose and approved with management oversight. For Microsoft 365 Applications any required access by Microsoft is for a limited time. Microsoft 365 applications implement and maintain multiple security measures for the protection of personal data as part of any data that are provided to Microsoft by EPO through use of the Microsoft 365 services, which encompass the following: organisation of information security (e.g., security ownership, security roles and responsibilities, risk management program), asset management (e.g. asset inventory and asset handling), human resources security (e.g. security training), physical and environmental security (e.g. physical access to facilities, physical access to components, protection from disruptions, component disposal), communications and operations management controls (e.g. operational policy, data recovery procedures, anti-malware controls, event logging), access control measures (e.g. access policy, access authorisation, least privilege, integrity and confidentiality, authentication, network design), information security

incident management (e.g. incident response process, service monitoring) and business continuity management. Microsoft also implements and maintain appropriate technical and organisational measures for protection of any other personal data distinct from the one described above, which are described in Microsoft Security Policy. Microsoft 365 applications have been configured to preserve the confidentiality of the information by employing the measures listed above. In addition, anonymous access is not authorised. Any information you add to Microsoft 365, be it via chat, videoconference, or file sharing, will be available only to the specific users and groups indicated in section 4 above. Microsoft 365 applications are certified in several security standards, including ISO27001, SOC1 Type II, SOC2 Type II and ISO27018 Code of Practice for Protecting Personal Data in the Cloud and complies with the requirements set forth in ISO27002. Microsoft conducts annual audits of the security of the computers, computing environment, and physical data centres that it uses in processing of personal data. The audits are performed by independent, third-party auditors according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework. Personal data is stored in the EU according to the application configuration implemented by the EPO. It may, however, be made available to subprocessors in other countries, depending on the requirements for maintenance, support or operation of cloud-hosted services, and the availability of this expertise. If access is granted, it is always temporarily and only to the data required for the specific maintenance, support or operation procedure being carried out. The following safeguards are implemented: • In all transfers to third countries, Microsoft uses EU Standard Contract Clauses for data transfer with its sub-processors. • Microsoft requires subprocessors to join the Microsoft Supplier Security and Privacy Assurance Program. This programme is designed to standardise and strengthen data handling practices, and to ensure that supplier business processes and systems are consistent with those of Microsoft. EPO-specific measures relating to the Exchange Online and Outlook: • EPO credentials via modern authentication are required in order to access the email inbox. • Access from devices which are not jointed to EPO's domain is subject to MFA. • Authentication and authorization based on roles. MFA is enforced to activate any roles. • Access reviews on existing roles; audit history.

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 232

Name Institutional issues and matters relating to the Legal division and the Unitary Patent Division - provision of legal advice

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 44 - General Administration

Entity Name - Controller (Entities) DG5 - 52 - Legal Affairs

External processors

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

OpenText

External processors	
Name OpenText	

Microsoft

External processors	
Name Microsoft	

Microsoft

External processors

Name	
Microsoft	

Description of the processing

Description Within Legal Affairs, D 5.2.3 Institutional Affairs, Legal and Unitary Patent Division provides legal advice in matters of the domain of expertise of the Directorate, often in the form of explanatory notes, legal opinions, internal notes, reports, drafts for legal texts, presentations, letters, speaking notes etc. (hereinafter “legal advice”).

Requests to this end are received from the hierarchy or other units of the Office, including concerning adequate response to requests for cooperation with:
- other International Organisations or
- competent authorities of the Contracting States or
- any other third party.

Requests are usually received at a generic email account of the Directorate (D523inst@epo.org; legaldivision@epo.org) or by the Director.

They lead to the opening of an electronic file in the case management system of the Directorate (CMS) under a specific file number together with the name of the requester and the employee(s) to whom the matter is assigned within the Directorate. Requests might also be stored in the Outlook accounts of the Directorate. A paper version of the file might also be opened.

Once assigned to a Directorate member, the matter and legal question is identified, assessed, and answered to the requester via e-mail, orally, in paper form or by giving access to the document on a shared drive.

The handling of matters in/by the Directorate might require the organisation and holding of phone calls, physical or virtual meetings. Language Services might be involved as necessary for translation or editing.

For certain matters, an external attorney at law will be involved to assist, who will act as a "controller" in relation to personal data possibly associated with a specific case. The choice of a law firm/its location will a.o. depend on the area of expertise required.

The relevant correspondence, drafts and final legal advice are saved in the CMS and email accounts of the Directorate, in the paper version if one was created and possibly in working files created by the employee dealing with the matter on storage places provided by the Office. For certain matters requiring consultation of other units or information and/or sign-off by hierarchy, relevant information and documents are shared via a specific document management system (CommonLog or OpenText).

Personal data associated with the handling of a given request can be transmitted or transferred, for example to private or public entities outside the EEA, or to international organisations, where necessary to achieve an adequate response to the request.

The active processing ends with the closure of the matter.

Archiving of documents after the end of the retention period, as provided in Article 14 DPR, is described in a dedicated record.

Legal opinions provided by external attorneys are kept separately in databases and storage places provided by the Office where are also kept documents concerning the work of the Directorate, such as minutes of meetings.

Purpose of Processing 3. This requires retaining previous legal advice for later reference to harmonise legal practice., 2. This encompasses ensuring proper collaboration, consultation, alignement and hierarchy's approval., 4. It is also necessary for planning and managing the activities of the directorate, including reporting and statistics., 1. The processing of personal data is necessary for providing legal advice on matters within the expertise of D 5.2.3, Institutional Affairs, Legal and Unitary Patent Division.

Data Retention After the closure of a matter, related files are kept for up to 20 years.

The retention period begins to run on 1 January of the year immediately following the date on which the file was closed. This approach might be revised once the available tools will allow for an automatic follow-up and handling of retention times.

Certain files/parts of the file (such as correspondence concerning relations and cooperation with Member States or International Organisation) with particular value are permanently preserved.

Data subjects and categories of personal data

Contractors

Matter/Log file	
Attachments	Metadata
General	
Any other information	Assessment and legal opinions
Input provided during the deliberation and decision-making process	
Ticketing	
Ticket related data	
Contact Information	
Contact Details	Phone Numbers
Working email address	
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Employment Information	
Assessment and legal opinions	Business Unit Division
Company Entity	Department name and/or number
Grievances and Complaints	
Personal Identification	
First Name	Full Name
Surname	

Employees

Matter/Log file	
Attachments	Metadata
General	
Any other information	Assessment and legal opinions
Input provided during the deliberation and decision-making process	
Ticketing	
Ticket related data	
Contact Information	
Contact Details	Phone Numbers
Working email address	
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Employment Information	
Assessment and legal opinions	Business Unit Division
Company Entity	Department name and/or number
Grievances and Complaints	
Personal Identification	
First Name	Full Name
Surname	

Externals

Matter/Log file	
Attachments	Metadata
General	
Any other information	Legal opinions and assessments
Ticketing	
Ticket related data	
Contact Information	

Contact Details	Phone Numbers
Working email address	
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Employment Information	
Company Entity	
Personal Identification	
First Name	Full Name
Surname	

Former Employees

General	
Legal opinions and assessments	
Contact Information	
Contact Details	
Personal Identification	
First Name	Full Name
Surname	

Recipient of the personal data

Recipients of the data The requester is usually a recipient.

Further recipients might be as described below, on a need to know basis and depending on the subject-matter of the request.

Within the EPOrg:
- Other units
- Hierarchy
- Administrative Council

when information or consultation is necessary to achieve one of the above mentioned purposes.

When recipients are outside the EPO, it is usually in the following circumstances:
- Attorney at law
- Addressee of a letter of content (e.g.: ILO, Ministry contact points in Host States...)

Furthermore, processors listed in point 1.8 are recipients.

Purpose of sharing The requester: to provide the advice sought.

Within the EPO
- Other units for information or consultation
- Hierarchy for information or approval
- Administrative Council for submission of CA documents

Outside the EPO:
- Attorney at law for obtaining legal services
- Addressee of a letter of content for information
- Processors: for technical support.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation
Occasionally to International Organisations, depending on the subject matter of a matter.

Transfer mechanism(s) The recipient provided appropriate safeguards, Derogation in accordance with Art. 10 DPR

Country where data might be transferred - Processor (Vendors)
OpenText - United Kingdom, Microsoft - United States, TRE Thomson Reuters - Luxembourg

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, International cooperation activities

Derogations Art. 10 DPR The transfer is necessary for the performance of a task in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning, or to perform obligations arising from its duty of co-operation with the contracting states

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 233

Name Legal practitioners' list and its maintenance

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG5 - 53 - Patent Law and Procedures

External processors

ServiceNow

External processors	
Name ServiceNow	

Microsoft

External processors	
Name Microsoft	

Microsoft

External processors	
Name Microsoft	

ServiceNow

External processors

Name	
ServiceNow	

Description of the processing

Description Legal practitioners may take over representation in proceedings established by the EPC in the same way as a professional representative registered on the list if they provide evidence that they fulfil the specific requirements as outlined in Article 134(8) EPC.

The Legal Division is responsible for the registration and deletion of legal practitioners in an internal database, based on the decision of the President of the European Patent Office dated 21 November 2013 concerning the responsibilities of the Legal Division, OJ EPO 2013, 600 and for entry in the European Patent Register, Rule 143(1)h EPC.
For his registration, the data subject must provide personal data like name, address, gender, accompanied by documents of proof/evidence of belonging to the bar.
Likewise, the deletion requires a request by the legal practitioner himself or others (e.g. dependants, bar association). For the processing of deletion, special documents are required depending on the grounds of the deletion. Such documents are e.g. a death certificate or bar association exclusion.
The processing of the aforementioned requests might necessitate the sharing of the data with other units within the EPO to address questions arising from the case at stake, e.g. of legal nature.
Besides, the Legal Division provides other units of the EPO with relevant information necessary to perform tasks associated with being registered as legal practitioner, e.g. to allow invitation to specific events, seminars, surveys etc. Other contact detail exports or statistics can be provided internally, on request.
In terms of workflows, the request for registration and any change of name, address or other details must be addressed to the responsible Legal Division. Documents are received by post, e-mail with attachment,
fax, filed in Madras (EPO internal electronic repository), Customer Service Management.

Data Retention For reasons of legal certainty, personal data is kept up to 99 years, starting from the first entry date on the list of legal practitioners.

Purpose of Processing 4. Preparation of statistics, 1. The processing of personal data is necessary for the setting up, maintenance and publication of the list of legal practitioners by the Office and providing up-to-date information to stakeholders as well as all associated actions to e.g. ensure a proper and efficient information flow and management of associated activities. This encompasses following elements:, 3. provide Office's units with information necessary to perform tasks associated with being listed as legal practitioners, 2. registration and deletion from the list of legal practitioners and use of this information by the Office for related actions taking place during the patent granting process including name publication in European Patent Register

Data subjects and categories of personal data

Externals

Ticketing	
Ticket related data	
Contact Information	
Contact Details	Phone Numbers
Working email address	
Professional Experience & Affiliations	
Professional Memberships	Qualifications Certifications

European Patent Register Data	
Address	Data provided by the data subjects
Correspondence	
Personal information provided voluntarily	
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications
Employment Information	
Business Unit Division	Company Entity
Job Title Role	Office Location
Personal Identification	
First Name	Full Name
Gender	Surname
Signature	

Employees

Ticketing	
Ticket related data	
Contact Information	
Phone Numbers	Working email address
Employment Information	
Business Unit Division	Job Title Role
Office Location	Personnel Number
Personal Identification	
Full Name	Gender

Recipient of the personal data

Recipients of the data Different business units at the EPO will have access to the information stored on the contact details database:

• DG0, DG1, DG5
• Other involvements are possible, e.g. Board of Appeals on a need-to-know basis

Purpose of sharing • DG1 as needed for the patent grant procedure
• Other internal contact detail exports or statistics on request for DG0, DG1, DG5, on a need to know basis
• Other involvements are possible, e.g. Board of Appeals in case of an appeal

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors)
Microsoft - United States, ServiceNow - Netherlands

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 234

Name User Consultation on Guidelines for Examination

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG5 - 53 - Patent Law and Procedures

External processors

Infotel Conseil SA

External processors	
Name Infotel Conseil SA	

Microsoft

External processors	
Name Microsoft	

Microsoft

External processors	
Name Microsoft	

Description of the processing

Description In the course of the annual revision of the Guidelines for Examination, an online user consultation is conducted by the delegated controller/D521. For these online consultations, personal data of the participants are collected.

Participation in the user consultation happens on a voluntary basis. Users are informed via, inter alia, the EPO's Official Journal, webnews items and social media platforms about the launch of the user consultation for filing any comments to the recently revised Guidelines. The comments must be filed via a webform on the EPO website.

Personal data is received and seen by a restricted number of EPO employees in the delegated controller's directorates.

After three months, all contributions to the consultation are anonymised, removing the ability to identify an individual and therefore destroying the personal data.

Purpose of Processing The user consultation serves to collect feedback on the Guidelines in force and suggestions for amendments, with a view to address and reflect the user's wishes and concerns in the practice of the Office. Personal data processed in this context permits relating individual comments, preference and wishes to specific users groups, thus allowing proper assessment of the relevance of the feedback.

Data Retention Personal data processed are stored for the period of time necessary to achieve the purpose for which they have been processed.

The personal data entailed in the user consultation will be deleted three months after the end of the consultation.

Data subjects and categories of personal data

Externals

General	
Answers to surveys, assessments or quizzes	Any other information
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Personal information provided voluntarily	
Employment Information	
Job Title Role	
Personal Identification	
Full Name	

Recipient of the personal data

Recipients of the data Access to the data is limited to the processor and to a resctricted number of staff in the delegated controller's units.

Infotel (platform for the survey)

All further sharing of information on the user consultation is on anonymous basis, i.e. do not allow to identify the participants and their answers.

Purpose of sharing Sharing the contributions and personal data of contributors with restricted number of staff from the delegated controller's units allows individual contributions to be attributed to specific user groups, for the sake of a proper assessment of the relevance of the feedback.
Infotel have access to the data as they provide the platform that collects the data.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards, Data Protection EU Comm Standard Contractual Clauses

Country where data might be transferred - Processor (Vendors) Microsoft - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 235

Name Associations' lists maintenance

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG5 - 53 - Patent Law and Procedures

External processors

ServiceNow

External processors	
Name ServiceNow	

Microsoft

External processors	
Name Microsoft	

Microsoft

External processors	
Name Microsoft	

ServiceNow

External processors

Name	
ServiceNow	

Description of the processing

Description Pursuant to Article 134(1) EPC representation of natural and legal persons in proceedings established by the EPC may only be undertaken by professional representatives whose names appear on a list maintained for this purpose of the EPO. Pursuant to Rule 152(11) EPC an authorisation of an association of representatives shall be deemed to be an authorisation of any representative who can provide evidence that he practises within that association. This legal fiction allows a party to authorise several representatives as an association instead of singly, provided this association is registered with the EPO.

The Legal Division of the EPO has sole responsibility for the registration and deletion of associations.

The requestor(s) must provide personal data like personal name, name and address of the association,
representative number and signature, entry or deletion dates (if these should deviate from the actual processing date of the EPO). The request is sent to the Legal Division, preferably using the dedicated EPO Forms, by post, e-mail and attachment, fax or are filed OLF options or via the Customer Service Management.

Other than the processing of registration, changes to or deletions of associations, the processing may also involve the sharing of data with other units within the EPO, as necessary to:
- address related questions arising in the patent grant process,
- perform tasks associated with being listed as member of an association, e.g. invitation to specific events, seminars, surveys etc. by the Academy,
- monitor developments in this area (e.g. statistics).

Data Retention For reasons of legal certainty, personal data is kept up to 99 years, starting from the deletion date of the association.

Purpose of Processing 3- Preparation of statistics, 2– registration, administration and deletion of associations and associated respective entries in the European Patent Register., 1. The processing of personal data is necessary for the registration, administration and deletions of associations by the EPO and providing up-to-date information to competent units in the patent grant process toensure a proper and efficient information flow and management of associated activities.

Data subjects and categories of personal data

Externals

General	
Any other information	
Ticketing	
Ticket related data	
Contact Information	
Contact Details	
Professional Experience & Affiliations	
Professional Memberships	
Representation in EPO's Patent Granting Process	

Affiliation to Association of professional representatives	All data provided upon request for entry or change
EPO CDS (Client Data System) categories related to the Representation role	Representative registration number (ID)
Supporting documentation	
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Personal information provided voluntarily	
Personal Identification	
First Name	Full Name
Surname	Signature

Employees

Ticketing	
Ticket related data	
Contact Information	
Phone Numbers	Working email address
Employment Information	
Business Unit Division	Job Title Role
Office Location	Personnel Number
Personal Identification	
Full Name	Gender

Recipient of the personal data

Recipients of the data Different business units at the EPO will have access to the information stored on the contact details database:

• DG0, DG1, DG5
• Other involvements are possible, e.g. Board of Appeals on a need-to-know basis

Purpose of sharing • DG1 as needed for the patent grant procedure
• Other internal contact detail exports or statistics on request for DG0, DG1, DG5, on a need to know basis
• Other involvements are possible, e.g. Board of Appeals in case of an appeal

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Country where data might be transferred - Processor (Vendors) ServiceNow - Netherlands, Microsoft - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Transfer mechanism(s)	Derogations Art. 10 DPR
The recipient provided appropriate safeguards	

Organisational and security measures

Organisational and security measures
EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 239

Name Dispute settlement activities in national proceedings or arbitration context

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 44 - General Administration

Entity Name - Controller (Entities) DG5 - 52 - Legal Affairs

External processors

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

OpenText

External processors	
Name OpenText	

External legal counsel/Law firm

External processors	
Name External legal counsel/Law firm	

IBM Notes

External processors

Name
IBM Notes

External Law Firms

External processors
Name
External Law Firms

Arbitration tribunal

External processors
Name
Arbitration tribunal

Microsoft

External processors
Name
Microsoft

Description of the processing

Description PD52 Legal Affairs is responsible for providing legal support in all kinds of domestic legal proceedings brought against the European Patent Organisation (EPOrg), and where the EPOrg is a party to arbitration proceedings. A dispute may be submitted to arbitration for example on the basis of an arbitration clause in a contract or following an ad hoc offer made by the EPOrg. Such alternative resolution is also offered to external data subjects in the situation envisaged in Art. 52 of the Data Protection Rules (DPR) (data protection arbitration).

To serve this purpose, personal data are processed at various stages of handling a case, of mainly the parties, their representatives, other participants in the proceedings in any capacity (such as experts, witnesses, bailiffs, judges...) or about third parties if for example their data are contained in the parties' submissions. Typically the data categories concerned in the course of handling a case include such data allowing identification and contact details of the persons above, as well as further information as necessary for providing legal support in the case (depending on the subject matter of the proceedings). The data are usually obtained from the exchange of submissions in a case, possibly also from internal fact-finding exercise/gathering of evidence or publicly available sources (e.g. internet, press).

The various stages will differ depending on the case and type of proceedings at stake. Typically involved operations on personal data upon handling a case are described below.

- For domestic legal proceedings:
A writ of summons is served by a bailiff or by letter. The Office's unit having received it, generally the President's office, forwards it to Legal Affairs.

- For arbitration proceedings:
Legal Affairs is involved from the formation of the arbitral tribunal.
For the specific case of data protection arbitration, a request is made

through an online form to the President of the Office, who forwards the request to the DPO, who then forwards the request to Legal Affairs. The request is sent to the Permanent Court of Arbitration acting as appointing authority for the appointment of an arbitrator.

- Upon opening of a case in Legal Affairs, the responsible lawyer(s) is assigned. An electronic case file is opened in the case management system of the directorate (CMS). In some cases a paper file might also be created.

- Legal Affairs assesses the claim and procedure at stake and advises the EPO's hierarchy. This legal support is provided for example in the form of explanatory notes, legal opinions, drafting submissions, emails and letters. This might require exchanging information with the hierarchy, the Administrative Council and/or other departments in the EPO, and/or with external law firms.

- The EPOrg is represented in the proceedings directly by Legal Affairs and/or by external law firms.

- Personal data are disclosed outside the Office as necessary for the conduct of the legal proceedings or arbitration (such as for the exchange of correspondence and submissions with opposing parties, with representatives, with national bodies or arbitral tribunal before which proceedings are pending).

- Correspondence and documents are stored in the CMS and email accounts of the directorate, in the paper file if one was created and possibly in electronic working files created by the employee dealing with the matter on storage places provided by the Office. As necessary for information, consultation or approval, documents or information related to a case are shared within the EPO using the usual internet channels such as Outlook, CommonLog, SharePoint and OneDrive Shared Drives.

- At the end of the procedure, Legal Affairs is involved in the implementation of measures to be taken to implement a court order or arbitral award, e.g. for payment of damages necessary data would be shared with relevant units to proceed with a payment.

- Once the last actions related to a case have been taken, the corresponding file(s) is closed and assigned an archive reference.

Archiving of documents after the end of the retention period, as provided in Article 14 DPR, is described in a dedicated record.

Data Retention After the closure of a matter, related files are kept for 20 years.

The retention period begins to run on 1 January of the year immediately following the date on which the file was closed. This approach might be revised once the available tools will allow for an automatic follow-up and handling of retention times.

Purpose of Processing - to manage the relationship with external attorneys and to monitor billing, - to ensure statistical monitoring of disputes, - to defend and represent the EPOrg in domestic legal proceedings or arbitration proceedings, including the availability of dispute files for later reference.

Data subjects and categories of personal data

Externals

Contact Information	
Contact Details	
Correspondence	
Additional Information which might be provided in the course of exchanges	Personal information provided voluntarily

Personal Identification	
First Name	Full Name
Surname	Nationality
Signature	

Employees

Contact Information	
Phone Numbers	Working email address
Employment Information	
Department name and/or number	
Personal Identification	
First Name	Full Name
Surname	

Recipient of the personal data

Recipients of the data Within the EPO:
- Hierarchy
- Other EPO units (e.g. Employment Law, Language Services)

When recipients are outside the EPO, it is usually in the following circumstances:
- Judicial body or other body before which proceedings are pending
- Arbitral tribunal
- Parties to the proceedings
- Representatives

Purpose of sharing Within the EPO:
- Hierarchy / for information and/or approval
- Other EPO units e.g. Contract Law or Employment Law / for consultation; Language Services / for editing or translation requests

Outside the EPO:
- Judicial body or other body before which proceedings are pending / for the conduct of proceedings
- Arbitral tribunal / for appointment of an arbitrator (Permanent Court of Arbitration) or for the conduct of proceedings
- Parties to the proceedings / for the conduct of proceedings
- Representatives / for the conduct of proceedings

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation For domestic legal proceedings: any body having jurisdiction in the case at hand.
For data protection arbitration: Permanent Court of Arbitration (for appointment of arbitrator).

Country where data might be transferred - Processor (Vendors) Microsoft - United States, OpenText - United Kingdom, TRE Thomson Reuters - Luxembourg

Reasons for the transfer Public Authorities/Government Bodies, Service provider, Conduct of proceedings

Transfer mechanism(s) The recipient provided appropriate safeguards, Derogation in accordance with Art. 10 DPR

Derogations Art. 10 DPR The transfer is necessary for the performance of a task in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning, or to perform obligations arising from its duty of co-operation with the contracting states, The data transfer is necessary for the establishment, exercise or defence of legal claims and their transmission is not precluded by agreements under international law or other applicable legal provisions of the European Patent Organisation

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 241

Name Central Fee Payment

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 41 - Finance, DG4 - 46 - CIO / BIT

Entity Name - Controller (Entities) DG4 - 41 - Finance

External processors

SAP

External processors	
Name SAP	

Financial Institutions

External processors	
Name Financial Institutions	

Ingenico

External processors	
Name Ingenico	

Description of the processing

Description Personal data is processed to enable the patent applicants, representatives and other parties to pay patent fees and claim refunds.

To use Central Fee Payment, you need to:
1) either register with an email address and a password for paying via credit card or using the bank transfer functionality or
2) directly sign in with the smart card, if you wish to pay with your deposit account. In this case the smartcard needs to be linked to your deposit account and have necessary access rights (pay fees online, view fees online or plan fees online). Smart card access rights are the same as in epoline and they are managed in epoline .

Contact information details are entered when you register to the service with an email address and a password, by filling the registration form. Only the fields marked with an asterisk are compulsory.

Once you have accessed the service, you can select the application and fees you would like to pay and add them to the shopping cart. At checkout, the fees are validated by the service. Afterwards, you can select the payment method: bank transfer, credit card or deposit account (deposit account only if logged-in with smart card).

Processing
EPO: from EPO side the payment process is automated.
Customer: Smart card users: the process is manual when they create their user profile for the first time. They choose fee for payment manually.
Non smart card users: the process is manual when they create their user profile for the first time. After registration the sign-in is with e-mail and password.

Data Retention If considered appropriate personal data can also be deleted if it can reasonably be expected that there is not operational need anymore. At a maximum years.

Purpose of Processing Enable patent applicants/representatives and other parties to pay patent fees and order and pay patent information products

Data subjects and categories of personal data

Externals

Applications' Log	
SAP Logs	
Contact Information	
Contact Details	Country
Home Address	Phone Numbers
Working email address	
Device Management Data	
Account ID	
Financial	
Bank Account Information	Bank Account Number

Credit Card Number	Debit Card Number
Deposit Account	
Browsing Information	
Cookie Information	
Personal Identification	
First Name	Surname

Recipient of the personal data

Recipients of the data European Patent Office: PD4.1.2 Revenue Controls

Outside EPO: Registered users have access to their own data

Purpose of sharing Enabling of online fee payment

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors) SAP - Germany, Ingenico - Unknown

Reasons for the transfer Financial Institution's intervention is necessary for the good performance of the Contract .

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement	More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 243

Name “MyEPO Portfolio” online service for parties to proceedings before the EPO (PGP)

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 46 - CIO / BIT, DG1 - 1 - Patent Granting Process

Entity Name - Controller (Entities) DG1 - 1 - Patent Granting Process, DG1 - 15 - Customer Journey and KAM

External processors

Okta Inc

External processors	
Name Okta Inc	

Description of the processing

Description MyEPO Portfolio is a web-based online service for parties to proceedings before the EPO that allows users to work with the EPO on portfolios of applications and patents. Users can:
• view application portfolios;
• view documents in the digital file;
• receive EPO Mailbox communications;
• perform procedural acts in response to communications from the EPO;
• file general authorisations and request changes and deletions thereof.

MyEPO portfolio also offers a "representative area", where professional representatives and persons authorised by them can:
• view their professional representative profile;
• request changes to their professional representative details;
• determine which contact details they wish to publish in the searchable database on the EPO website;
• request deletion from the list of professional representatives;
• request entry into the list of professional representatives;
• request registration and deletion of, and changes to, an association;
• view the information related to an association;
• file general authorisations and request changes and deletions thereof.

MyEPO Portfolio also provides access, procedural guidance and enables the exchange of digital information.

Personal data are processed for the purposes of MyEPO Portfolio services when conducting patent-grant and related proceedings (PGP) pursuant to the EPC and the provisions applicable under it, and likewise proceedings under the Patent Cooperation Treaty (PCT) and the Unitary Patent Rules (UPR).

Personal data are processed on the basis of Article 5a DPR (processing is necessary for the performance of a task carried out in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the EPO's management and functioning) and Article 5b DPR (processing is necessary for compliance with a legal obligation to which the controller is subject).

In particular, personal data are processed for the purposes of the EPO's task under Article 4(3) EPC of granting European patents, as further specified in the relevant provisions of the EPC and the other provisions applicable under it. Where these data are required for proceedings under the EPC, their processing is mandatory (mandatory personal data). The same applies mutatis mutandis to data required for proceedings under the PCT and the UPR.

Concerning the processing of personal data in proceedings related to European patents with unitary effect, reference is made to the Decision of the President of the European Patent Office dated 7 December 2022.

Personal data are collected when users perform procedural tasks or file procedural requests in MyEPO Portfolio. Depending on the nature of the task or procedural request, a task may appear in the Patent Work Bench (PWB) for a formalities officer to review and further process the task or request.

MyEPO Portfolio provides an administration facility. The designated company administrator can use this facility to grant access rights to company staff members. These rights include administration rights, the right to pay fees, and access to the Mailbox as well as to the company's portfolio of applications and patents.

The personal data are also processed using the PGP back-office systems allowing EPO staff to:
• process applications and patents pursuant to the EPC, the PCT, the UPR and the provisions applicable under them;
• conduct opposition proceedings and proceedings before the Legal Division;
• communicate with parties to the proceedings and, where applicable, third parties;
• maintain the European Patent Register for information of, and inspection by, any third party;
• draw up reports and statistics;
• exchange data with EPC, PCT, and/or UPR contracting states and with WIPO as part of co-operation projects and activities.

Relating to the purpose of sharing, please also see the detailed information about the specifics of the PGP procedures published in the Decision of the President of the European Patent Office dated 13 December 2021 concerning the processing of personal data in patent-grant and related proceedings (OJ EPO 2021 A98).

The personal data is also processed for the purpose of providing functions in the "representative area". The representatives can request entry onto the list of professional representatives before the EPO, for which their identities will be verified, and maintain their entries on the list of professional representatives through the self-service

Purpose of Processing Please see the detailed information regarding data processing under UPR in the Decision of the President of the European Patent Office dated 7 December 2022 concerning the processing of personal data in proceedings related to European patents with unitary effect., Personal data are processed for the purposes of MyEPO Portfolio services when conducting patent-grant and related proceedings (PGP) pursuant to the EPC and the provisions applicable under it, and likewise proceedings under the Patent Cooperation Treaty (PCT) and the Unitary Patent Rules (UPR). Personal data are collected when users perform procedural tasks or file procedural requests in MyEPO Portfolio. Depending on the nature of the task or request, the data may be subject to further processing by EPO staff. MyEPO Portfolio provides an administration facility. The designated company administrator can use this facility to grant access rights to company members. These rights include administration rights, the right to pay fees, and access to the Mailbox as well as to the company's portfolio of applications and patents. The personal data entered are further processed by EPO staff in order to: · process applications and patents pursuant to the EPC, the PCT, the UPR and the provisions applicable thereunder; · conduct opposition proceedings and proceedings before the Legal Division; · communicate with parties to the proceedings and, where applicable, third parties; · maintain the European Patent Register for information of, and inspection by, any third party; · draw up reports and statistics; · exchange data with EPC, PCT and/or UPR contracting states and with WIPO as part of co-operation projects and activities. Relating to the purpose of processing data, please also see the detailed information about the specifics of the PGP procedures published in the Decision of the President of the European Patent Office dated 13 December 2021 concerning the processing of personal data in patent-grant and related proceedings (OJ EPO 2021 A98). The personal data is also processed for the purpose of providing functions in the "representative area". The representatives can request entry onto the list of professional representatives before the EPO, for which their identities will be verified, and maintain their entries on the list of professional representatives through the self-service functionality in the representative area. The processing is not intended to be used for any automated decision-making, including profiling.

functionality in the representative area.

The processing is not intended to be used for any automated decision-making, including profiling.

Personal data will not be transferred to recipients outside the EPO which are not covered by Article 8(1), (2) and (5) DPR unless an adequate level of protection is ensured. In the absence of an adequate level of protection, a transfer can only take place if appropriate safeguards have been put in place and enforceable data subject rights and effective legal remedies for data subjects are available, or if derogations for specific situations as per Article 10 DPR apply.

The data is processed in line with the relevant provisions of the EPC, in particular:

• Applicant's name (i.e. family name and given names), address, nationality and state of residence or principal place of business (Rule 41(2)(c) EPC)
• Applicant's fax and phone numbers, where provided (Rule 41(2)(c) EPC)
• Applicant's signature (Rule 41(2)(h) EPC)
• Name of any representative, their signatures, address of their place of business (Rules 143(1)(h), 41(2)(d), 92(2)(c) EPC) and, where provided, representative number, association number, fax and phone numbers
• Inventor's name and country and place of residence (Rule 19(1) EPC)
• Personal data contained in copies of previous applications where applicants claim their priority (Rule 53(1) EPC)
• Name of the person making a payment and personal data relating to deposit accounts or other payment means (bank accounts, credit cards, etc.) (Article 6(1) RFees, Article 5(2) RFees together with the Arrangements for Deposit Accounts)
• Where applicable, any personal data relating to third-party observations, evidence, prior art, IT tools and services and oral proceedings
• Any other personal data provided by a party during the proceedings

Data Retention A patent provides a legal protection for 20 years, and there is no limitation to how long the post-grant procedures can last: after the patent granting procedure, there can be an opposition procedure which will review the patent granting procedure and involve members of the examining division. These members need to be able to retrieve their actions and comments. Moreover, after the patent granting procedure, there can be an appeal procedure whose outcome can be to reopen the examination procedure by the examining division. After that, revocation and limitation procedures may take place at any time, even after expiry of the patent protection. The examining division needs to be able to retrieve the actions and comments of the initial procedure. For more information, see the Decision of the President of the European Patent Office dated 13 December 2021 concerning the processing of personal data in patent-grant and related proceedings (OJ EPO 2021 A98).

Personal data used which is part of the patent grant procedure is stored indefinitely.

Personal data entered into and available in the “representative area” are stored in accordance with the Data protection statement on the processing of personal data within the context of the administration of the list of professional representatives before the European Patent Office and the Data protection statement on the processing of personal data in the context of the maintenance of the list of associations; personal data collected and available in relation to general authorisations are stored in accordance with the Data protection statement on the processing of personal data within the context of the administration of general authorisations.

In the event of a formal appeal/litigation, all data held at the time the formal appeal/litigation was initiated will be retained until the proceedings have been closed.

Data subjects and categories of personal data

Externals

General	
Any other information that complies with the terms and conditions of the service	
Contact Information	
Contact Details	Country
Home Address	Mobile Phone Number
Personal Email	Phone Numbers
Private Phone Number	Working email address
European Patent Register Data	
Address	
Device Management Data	
Account ID	
Representation in EPO’s Patent Granting Process	

Affiliation to Association of professional representatives	All data provided upon request for entry or change
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of a patent (claims, description, drawings, abstract)
Personal data potentially included within the content of patent procedure related information and publications	
Financial	
Bank Account Information	Bank Account Number
Credit Card Number	Debit Card Number
Employment Information	
Company Entity	Corporate Credit or Debit Card Numbers
Department name and/or number	Job Title Role
Language preference (of communication)	Office Location
Personal Identification	
Digital signature	First Name
Full Name	Surname
Nationality	Signature
User Account Information	
Account Number	Account Password
User ID	
Government Identifiers	
ID/Passport picture	National Identity Card Details
Passport Number	
System Logs	
Audit Logs (a.k.a. Audit Trail)	

Recipient of the personal data

Recipients of the data Personal data are processed by the departments of the EPO specified in Article 15(a) to (e) EPC. This includes EPO staff involved in:
• carrying out the procedures laid down in the EPC, PCT and UPR;
• providing user and technical support;
• improving the patent grant process and MyEPO Portfolio services.

The personal data are disclosed on a need-to-know basis to the EPO staff working in DG1 Patent Granting Process, Boards of Appeal, DG4 Business Information Technology and DG5 Legal Affairs.

External contractors involved in providing, maintaining and offering support for My EPO Portfolio services may also process personal data, which can include accessing it.

Personal data will only be shared with authorised persons responsible for the necessary processing operations. They will not be used for any other purposes or disclosed to any other recipients.

Purpose of sharing Personal data are processed by the departments of the EPO specified in Article 15(a) to (e) EPC. This includes EPO staff involved in:
• carrying out the procedures laid down in the EPC, PCT and UPR;
• providing user and technical support;
• improving the patent grant process and MyEPO Portfolio services.

See the detailed information about the specifics of the PGP procedures published in the Decision of the President of the European Patent Office dated 13 December 2021 concerning the processing of personal data in patent-grant and related proceedings (OJ EPO 2021 A98).

In general, data transfers do not take place, with the following exceptions: registered users from parties to PGP proceedings can download personal data from MyEPO Portfolio for patent applications and patents to which they have access rights. Appropriate levels of access are granted individually to the above-mentioned recipients only.

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors) Okta Inc - Costa Rica, Okta Inc - United States

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, MyEPO Portfolio is hosted on the EPO's premises, and the following base security measures generally apply: • user authentication and access control (e.g. role-based access control to the systems and network, principles of need-to-know and least privilege); • logical security hardening of systems, equipment and network; • physical protection: EPO access controls, additional access controls to datacentre, policies on locking offices; • transmission and input controls (e.g. audit logging, systems and network monitoring); • security incident response: 24/7 monitoring for incidents, on-call security expert. We take appropriate technical and organisational measures to safeguard and protect your personal data from accidental or unlawful destruction, loss or alteration and unauthorised disclosure or access., For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 244

Name European, international and PCT related legal advice (D 5.2.2)

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG5 - 52 - Legal Affairs

External processors

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

OpenText

External processors	
Name OpenText	

OpenText

External processors	
Name OpenText	

Microsoft

External processors	
Name Microsoft	

Microsoft

External processors	
Name Microsoft	

Description of the processing

Description D 5.2.1 receives requests from the hierarchy, other units of the Office or external parties seeking advice in matters of the domain of expertise of the Directorate (i.e. Patent Developments and IP Lab), to be provided in the form of explanatory notes, legal opinions, internal notes, reports, drafts for legal texts, presentations, letters, speaking notes etc. (hereinafter “legal advice”). This includes requests and processing of personal data to cooperate with:
- other Organs of the European Patent Organisation (Administrative Council),
- other International Organisations or
- competent authorities of the Contracting States

Requests are usually received at a generic email account of the Directorate or by the Director. They lead to the opening of an electronic file in the case management system of the Directorate (CMS) under a specific Log number together with the name of the requester and the case handler to whom the case is assigned within the Directorate. Requests might also be stored in the outlook accounts of the directorate (generic email account). A paper version of the file might also be printed.

Once assigned to a team member, the matter and legal question is identified, assessed, and answered to the requester via e-mail, orally, in paper form or by giving access to the document on a shared drive. The handling of matters in/by the Directorate might also require the organisation and holding of phone calls, physical or virtual meetings. D521 might involve an attorney at law. The relevant correspondence, drafts and final legal advice are saved in the CMS and, the case be, in a generic email account of the directorate.

The active processing ends with the closure of the case.

Data Retention Personal data for non patent-file related matters is kept for the default retention time period for legal advice of Legal Affairs (provided in the Mattersphere Case Management System record) except for cases where e. g. President, Vice President or other high ranked Officers were involved in order to be able to document the decision-making process.

Personal data in patent-file related matters (European patent applications and European patents) should be kept for thirty years to cover the longest possible period under Rule 147 EPC.

The said retention periods will be applied as follows: When a file having reached the end of the retention period is consulted by a staff member, it will be anonymised or destroyed. This approach will be revised once the available tools will allow for an automatic follow-up and handling of retention times.

Purpose of Processing The processing of personal data is necessary for providing advice on matters within the expertise of the directorate. This encompasses: (i) Questions of legal nature, (ii) advising and supporting on confidential deliberations and decision-making of the Office, (iii) provide up-to-date information to stakeholders as well as taking associated actions to e. g. ensure a proper and efficient information flow and management of associated activities, (iv) promoting the legal framework of the Organisation, also through awareness raising, (v) Handling with requests outside the direct expertise, if requested by senior management, (vi) planning and managing the activities of the directorate, including statistics, (vii) enabling the availability of previous advice for later reference in the event of subsequent related request or litigation, and (viii) archiving and statistical purposes.

Data subjects and categories of personal data

Employees

General

Any other information	
Contact Information	
Phone Numbers	Working email address
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Personal information provided voluntarily	
Employment Information	
Business Unit Division	
Personal Identification	
Full Name	

Externals

General	
Any other information	
Contact Information	
Phone Numbers	Working email address
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Personal information provided voluntarily	
Employment Information	
Company Entity	Job Title Role
Office Location	
Personal Identification	
Full Name	

Recipient of the personal data

Recipients of the data - The requestor
- PD52 Hierarchy
- Other units or external parties
- The external processors

Purpose of sharing Data is shared with the requestor in order to deliver the legal advice requested.

Data is shared with hierarchy and other units when information or consultation is necessary to achieve one of the above mentioned purposes.

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards, EC Adequacy Decision

Country where data might be transferred - Processor (Vendors) Microsoft - United States, TRE Thomson Reuters - Luxembourg, OpenText - United Kingdom

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 246

Name Archives Legal Affairs

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG5 - 52 - Legal Affairs

External processors

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

iron mountain

External processors	
Name iron mountain	

Description of the processing

Description Legal Affairs archives files with permanent institutional or legal value for PD52 operations.

This record covers the processing operations of personal data related to this archiving*.

The personal data is archived in:
1) the paper based archive, where paper documents (including files) have been classified along a dedicated nomenclature. Legal Affairs' staff is granted access by the archivist, on a need-to-know basis.
2) the electronic archive, made of the electronic files and documents from Legal Affairs' Case Management System (CSM) which are being kept after the elapsing of the retention period. The files are stored separately for each directorate within Legal Affairs. Access is to be restricted to the staff of the corresponding directorate, on a need-to-know basis.

This approach will be revisited when the available tools will provide automated and differentiated means to e.g. identify, anonymize and/or pseudonymize the personal data.

*Archiving in the meaning of the DPR. It refers to the data kept after the elapsing of the retention period. For the storage of personal data until the elapsing of the retention period(s), it is referred to the relevant record(s) of processing operation.

Data Retention All processing operations under the responsibility of the delegated controller are described in the relevant records of processing operation, which state the applicable retention period(s). This archive record describes the way the personal data is kept/archived, should it not be destroyed at the end of the applicable retention period.

Purpose of Processing Archiving of documents of permanent institutional or legal value for Legal Affairs' operations.

Data subjects and categories of personal data

Employees

Applications' Log	
SAP Logs	
Social	
Social Media Account	Social Media Contact
Social Media History	
Sensory and Electronic Information	
Audio Information	Electronic Information
Presence Status	Thermal Information
Time stamps from their access to the buildings	Visual Information
Building area and site	
Building area and site	
Representation in EPO's Patent Granting Process	

Representative registration number (ID)	
Telephony Interaction Data	
Telephony Session Content	Telephony Session Details
Telephony Session Metadata	
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name
Gender	Height
Surname	Marital Status
Nationality	Picture
Racial or Ethnic Origin	Religion/Religious Beliefs
Sexual Orientation	Signature
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
Project management experience	
General	
Any other information	Assessment and legal opinions
Input provided during the deliberation and decision-making process	Legal opinions and assessments
Nomination justificative	Personal Information in SAP
Sensitive Personal Data in SAP	Special Categories of Data in SAP
User association	
Workplace Welfare	

Records of Personal Properties	
Contact Information	
Contact Details	Country
Emergency Contact Details	Home Address
Home Leave Address	Mobile Phone Number
Personal Email	Phone Numbers
Previous Residence Address	Private Phone Number
Teleworking address	Working email address
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
Diagnostic tools' results	IDP
Instructor related data	Learning external events
Learning history	Learning plan
Ratings	Social learning inputs
Device Management Data	
Account ID	AppleID for iOS/iPadOS Devices
Azure Active Directory Device ID	EAS Device ID
Encryption Keys	Intune Device ID
Intune Device Management ID	Last Logon Time
MAC Address	Managed Application Device Tag
Managed Application ID	Platform-specific IDs
Tenant ID	Windows ID for Windows Devices
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Patent Process Related Data	

Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of a patent (claims, description, drawings, abstract)
Personal data potentially included within the content of patent procedure related information and publications	
Health Insurance Information	
Insurance Policy Information	Unique Identifier for Subscriber
System Logs	
Audit Logs (a.k.a. Audit Trail)	File data (name, size and/or hash)
Firewall/Router/Switch Logs	Ports
Registry data	Running Processes
System-, Application-, Security-related Server Logs	Transaction-related Details
Web Servers Logs	
Phone Call Information	
Called Phone Number	Caller's Phone Number
Phone Call Date and/or Time	Phone Call Duration
Phone Call Interaction History	Phone Calling History
Ticketing	
Ticket related data	
Physical and/or Digital Identifiable Assets	
Digital Certificate	ICCID (Integrated Circuit Card Identification Number)
IMEI Number (International Mobile Equipment Identity)	Mobile Device Name
Mobile Device Serial Number	Mobile Device's Network Adapter MAC Adress
Operating System Version	Smart Card Number
Videoconference Room/Equipment Identifier	Workstation Serial Number
Workstation's Hostname (Physical or Virtual)	Workstation's Network Adapter MAC address
Biometric	
Body temperature	Facial Recognition
Fingerprint	Voice Recognition
Online invigilation data	

Audio input	Webcam captures
Background Checks	
Criminal History	Criminal Records
Drug Test Results	Reference or Background Checks
Employment Information	
Active/Inactive Indicator	Appeals Records Information
Assessment and legal opinions	Benefits and Entitlements Data
Business Unit Division	Company Entity
Contract Type	Corporate Credit or Debit Card Numbers
Department name and/or number	Disciplinary Action
Duration of employment	End Date
End Date and Reason for Termination	EPO access badge number
Exit Interview and Comments	Grade
Grievances and Complaints	Hours of Work
Job Application Details	Job Group
Job Title Role	Language preference (of communication)
Line Reporting Manager	Membership in a EPO Staff Committee
Military Status	Office Location
Performance Rating	Personnel Number
Previous Work History	Record of Absence/Time Tracking/Annual Leave
Record of Maternity Leave	Rewards history
Room Number	Salary
Start Date	Weight
Unknown	
EPO badge validity	Identification of which membership is envisaged
Price list for discounts	
Geolocation	

Geolocation Information	
Network/application Interaction Data	
Results on phishing attempts (entered credential not processed)	Session content
Session details	Session metadata
Health Data	
Dietary requirements	Health Data
Mobility needs	
Professional Experience & Affiliations	
Affiliation	CV
Entry or deletion date as member of an association	Political Affiliation and Activities
Professional Memberships	Qualifications Certifications
Trade Union Membership	
Examination content data	
Examination marks	Examination result
Family Information	
Child’s Level/Year of Studies	Child’s School Enrolment Date Start
Children's Names	Child's birthday
Composition of the family (number of dependent children/persons)	Parents' Names
Spouse's information	Spouse's name
Financial	
Bank Account Information	Bank Account Number
Bank Statements	Bonus Payments
Compensation Data	Credit Card Number
Credit History	Debit Card Number
Fund Reservation Requests	Information on home loans
Insurance Information	Routing Number
Browsing Information	

Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
Category	Cookie Information
IP Address	Network Interaction History
URL	Website History
User Account Information	
Account Age	Account Number
Account Password	Membership Permissions
Ownership Permissions	Password
Password Hash	Third-party User Identifier
User ID	
Government Identifiers	
Car registration documents	Driving Licence Number
National Identification Number	National Identity Card Details
Passport Number	Social Security Number

Externals

Applications' Log	
SAP Logs	
Social	
Social Media Account	Social Media Contact
Sensory and Electronic Information	
Audio Information	Electronic Information
Presence Status	Time stamps from their access to the buildings
Visual Information	
Building area and site	
Building area and site	
Representation in EPO's Patent Granting Process	

Affiliation to Association of professional representatives	All data provided upon request for entry or change
Authorisee function	Authorisor function
EPO CDS (Client Data System) categories related to the Representation role	Representative registration number (ID)
Role in the Patent Grant Procedure	Supporting documentation
Telephony Interaction Data	
Telephony Session Content	Telephony Session Details
Telephony Session Metadata	
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name
Gender	Surname
Nationality	Picture
Signature	
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
Project management experience	
Matter/Log file	
Attachments	Metadata
General	
Answers to surveys, assessments or quizzes	Any other information
Input provided during the deliberation and decision-making process	Legal opinions and assessments
Nomination justificative	User association

Contact Information	
Contact Details	Country
Emergency Contact Details	Home Address
Mobile Phone Number	Personal Email
Phone Numbers	Private Phone Number
Working email address	
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
IDP	Instructor related data
Learning external events	Learning history
Learning plan	Ratings
Social learning inputs	
European Patent Register Data	
Address	Data provided by the data subjects
Device Management Data	
Account ID	AppleID for iOS/iPadOS Devices
Azure Active Directory Device ID	EAS Device ID
Encryption Keys	Intune Device ID
Intune Device Management ID	Last Logon Time
MAC Address	Managed Application Device Tag
Managed Application ID	Platform-specific IDs
Tenant ID	Windows ID for Windows Devices
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of a patent (claims, description, drawings, abstract)

Personal data potentially included within the content of patent procedure related information and publications	
System Logs	
Audit Logs (a.k.a. Audit Trail)	File data (name, size and/or hash)
Firewall/Router/Switch Logs	Ports
Registry data	Running Processes
System-, Application-, Security-related Server Logs	Transaction-related Details
Web Servers Logs	
Phone Call Information	
Called Phone Number	Caller's Phone Number
Phone Call Date and/or Time	Phone Call Duration
Phone Call Interaction History	Phone Calling History
Ticketing	
Ticket related data	
Physical and/or Digital Identifiable Assets	
Digital Certificate	ICCID (Integrated Circuit Card Identification Number)
IMEI Number (International Mobile Equipment Identity)	Mobile Device Name
Mobile Device Serial Number	Mobile Device's Network Adapter MAC Adress
Operating System Version	Smart Card Number
Videoconference Room/Equipment Identifier	Workstation Serial Number
Workstation's Hostname (Physical or Virtual)	Workstation's Network Adapter MAC address
Biometric	
Facial Recognition	Voice Recognition
Online invigilation data	
Audio input	Webcam captures
Employment Information	
Active/Inactive Indicator	Business Unit Division

Company Entity	Contract Type
Corporate Credit or Debit Card Numbers	Department name and/or number
Duration of employment	End Date
EPO access badge number	Hours of Work
Job Title Role	Language preference (of communication)
Membership in a EPO Staff Committee	Office Location
Previous Work History	Record of Maternity Leave
Unknown	
EPO badge validity	Identification of which membership is envisaged
Price list for discounts	
Network/application Interaction Data	
Session content	Session details
Session metadata	
Health Data	
Dietary requirements	Health Data
Mobility needs	
Professional Experience & Affiliations	
Affiliation	CV
Entry or deletion date as member of an association	Political Affiliation and Activities
Professional Memberships	Qualifications Certifications
Examination content data	
Examination marks	Examination result
Financial	
Bank Account Information	Bank Account Number
Bank details	Credit Card Number
Debit Card Number	Fund Reservation Requests
Information on home loans	Insurance Information

Browsing Information	
Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
Category	Cookie Information
IP Address	Network Interaction History
URL	Website History
User Account Information	
Account Age	Account Number
Account Password	Membership Permissions
Ownership Permissions	Password Hash
Third-party User Identifier	User ID
Government Identifiers	
ID/Passport picture	National Identity Card Details
Passport Number	

Recipient of the personal data

Recipients of the data - Employees of the delegated controller's units
- Other stakeholders

Purpose of sharing - Employees of the delegated controller's units: Access on a need to know-basis, i.e. when dealing with a matter in connection with the archived file concerned, requiring access to the archived file.
- Other stak: Depending on the particular circumstances of a case, it might be necessary to share information outside the delegated controller's unit.

Transfer

Transfer No

Country where data might be transferred - Processor (Vendors) TRE Thomson Reuters - Luxembourg

Transfer to public authority and/or International Organisation

Reasons for the transfer

Transfer mechanism(s)

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 247

Name Mattersphere Case Management System in Legal Affairs/PD5.2

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG5 - 52 - Legal Affairs

External processors

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

Description of the processing

Description The delegated controller/Legal affairs uses the software "mattersphere", a case management, knowledge database, electronic storage and archiving system (hereinafter “CMS”) from Thomson Reuters.

Each Directorate within the delegated controller's unit has an own area in the CMS which is not accessible by other directorates within or outside Legal Affairs. Each directorate can open new cases (so-called log files or matters) which are used to assign working requests to members (case handlers) of the relevant teams, gather the relevant information, document the elaboration of inputs.

The log files entail mainly:
1) a page with key information on each case (so-called metadata) entered in pre-defined fields, such as subject matter, requester's name and contact details, case handler within the unit, line managers of case handler, unit concerned, matter type.
2) attachments (such as email exchanges, documents, drafts, legal opinions).

At the end of the applicable retention period, the relevant files are either destroyed (deleted), anonymised or archived (archiving activities are described in a separate record).

Purpose of Processing The purpose of the processing is electronic case- knowledge- storage- and archive management in Legal Affairs. This encompasses the need to: 1. ensure proper preparation of subsequent actions e.g. further communications, proceedings, final decision; 2. preparation of statistics and overview for reporting/statistical purposes 3. retrieval of previous advice as precedence, example and reference when dealing with new requests, and with a view to harmonise internal and external practice for archiving purposes (archiving is subject of a separate record).

Data Retention The default retention period applicable for the personal data/documents entailed in the CMS is 20 years, unless a different retention period is mentioned in a specific record of processing operations of PD 5.2. Legal Affairs (the applicable data retention schemes depend on the type of personal data processed and the purpose of that processing).

The retention period usually begins to run on 1 January of the year immediately following the date on which the file was closed.

In the event of a formal appeal/litigation, all data held at the time when the formal appeal/litigation was initiated will be kept until the proceedings have been concluded or for the default retention period of 20 years, whichever period is longer.

This retention period applies without prejudice to possible archiving (archiving activities are addressed in a separate record).

Data subjects and categories of personal data

Employees

Matter/Log file	
Attachments	Metadata
General	
Any other information	Assessment and legal opinions
Legal opinions and assessments	
Ticketing	
Ticket related data	
Contact Information	
Contact Details	
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Employment Information	
Appeals Records Information	Assessment and legal opinions
Business Unit Division	Department name and/or number
Grievances and Complaints	

Externals

Matter/Log file

Attachments	Metadata
General	
Any other information	Input provided during the deliberation and decision-making process
Legal opinions and assessments	
Ticketing	
Ticket related data	
Contact Information	
Contact Details	
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily

Recipient of the personal data

Recipients of the data The content of the CMS is only accessible to the staff of the relevant directorate, within the delegated controller's unit.
If any sharing of information entailed in the CMS is necessary outside the delegated controller's unit, it is not done via providing access to the file in CMS.
Circumstances and ways of sharing depend on the different types of case/personal data processing and their purposes, as described in the records dedicated to the different types of processing.

Purpose of sharing Need to know.

Transfer

Transfer No

Country where data might be transferred - Processor (Vendors) TRE Thomson Reuters - Luxembourg

Transfer to public authority and/or International Organisation

Reasons for the transfer

Transfer mechanism(s)

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 249

Name Personal data processing related to team and service quality management in the interpreting area

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 41 - Finance, DG4 - 47 - Procurement and Vendor Management

Entity Name - Controller (Entities) DG4 - 44 - General Administration

External processors

UNITARY PATENT COURT

External processors	
Name UNITARY PATENT COURT	

Description of the processing

Description Interpreter groups: The EPO employs conference interpreters for EPO languages (“Group 1”) and occasionally for non-EPO languages (“Group 2”). They primarily interpret online oral proceedings via a web platform from their professional domiciles, and occasionally at in-person meetings in Munich. The EPO employs up to 230 interpreters for EPO languages, who handle more than 99% of the assignments, including Administrative Council meetings. Quality is monitored by the Team Manager Interpreting and the Director Language Services, who are advised by the Quality Management (QM) team of senior interpreters.
Interpreters for non-EPO languages (Group 2) handle less than 1% of assignments, mainly for ad hoc visits, annual events, or cooperation meetings such as IP5. There is no onboarding or accreditation process for this group.
I. Selection and onboarding
Interpreters for EPO languages (Group1) apply by submitting their bid to Procurement via the Dynamic Purchasing System (DPS). Qualified candidates are awarded framework contracts, setting out the general conditions for the provision of interpreting services. Depending on the demand for interpreting per language combination and the development of the EPO’s pool of interpreters, candidates may instead be kept on a waiting list for up to 5 years. Candidates allowed to start onboarding go through an onboarding process that includes

unpaid e-learning, mentoring, dummy booth practice and induction tests by the QM team. Candidates successfully passing induction tests enter a test phase during which they receive paid assignments and feedback from the QM team. Members of the QM team may also recommend them for accreditation: at the end of the test phase, the EPO decides whether to accredit an interpreter or not. Only accredited interpreters will be eligible for further interpretation work. The interpreters who fail to be accredited will receive general feedback on their performance, before the termination of the contract.
Accreditation is granted by the Director of Language Services on the basis of the advice of the Accreditation Board, which additionally consists of the Team Manager and two members of the QM team per language.
II. Quality management
To ensure high-quality interpreting services, Group 1 interpreters receive regular feedback:
a) During the phase prior to accreditation: Feedback from the QM team is processed using MS Forms and sent via a restricted LS email account (qm_interpreting@epo.org) to the interpreter concerned who has the possibility to reply to the feedback given - and to the restricted LS email account (Access: Director, Team Manager, 2 team members responsible for the process).
b) Peer Feedback: Accredited interpreters receive verbal feedback from colleagues, with organisational details (who to whom) stored in MS Forms/Excel file on OpenText. (Access to these details in Excel: Director, Team Manager, 2 team members responsible for the process).
These organisational details are sent by email to the interpreter concerned who has the possibility to reply to it.

c) Spot Check Feedback: Feedback from the QM team's spot checks of accredited interpreters is processed using MS Forms and sent via a restricted email account (qm_interpreting@epo.org) to the interpreter concerned who has the possibility to reply to the feedback given - and to the restricted LS email account (Access: Director, Team Manager, 2 team members responsible for the process).
III. Data regarding fees and travel expenses
Fees and travel expenses for interpreters are processed through the Interpreter Administration System (IAS). Interpreters receive weekly self-billing invoices covering their fees and travel expenses, to which they can add any supporting documents for travel. The Interpreting and Central Support staff review and complete this information. The interpreters then approve the final invoice, which is sent to SAP for further processing. In SAP, another team member conducts a final check before forwarding the invoice to Finance for payment. Processing is partly automated.

Data Retention 12 years

Purpose of Processing The personal data of interpreters engaged at the EPO under framework contracts are processed for the purpose of providing the EPO with the services of interpreters of the highest standard of ability, efficiency and integrity. The processing of personal data is necessary for: - keeping a pool of accredited and appropriately qualified interpreters; - service provision; - quality management purposes (induction of newly selected candidates and ensuring service quality) - administering the payment process. Legal basis: Rule 4 EPC.

Data subjects and categories of personal data

Externals

Contact Information	
Contact Details	Home Address
Mobile Phone Number	Working email address
Professional Experience & Affiliations	
CV	Qualifications Certifications

Financial	
Bank Account Information	Insurance Information
Employment Information	
Previous Work History	
Personal Identification	
Date of Birth	Full Name
Gender	Nationality
Education & Skills	
Education and Training History	Educational Degrees
Languages	

Recipient of the personal data

Recipients of the data 1) Access to applications
Interpreter application documents are made accessible to the following people in Language Services for the purpose of bid evaluation:
- the Language Services Director,
- the Team Manager Interpreting and Central Support
- the Interpreting and Central Support staff responsible for this process

2) Access to data in the IAS
- to Interpreting and Central Support staff to assign interpreters to meetings, send work offers, process the invoices and generate reports. It is accessible to the Interpreting and Central Support staff members responsible for interpreter administration, the Language Services Director, the Team Manager and the application manager. EPO external technicians involved in the organisation of oral proceedings have restricted access to IAS Internal. They can only view the weekly overviews (names of interpreters assigned to the respective oral proceedings, data concerning the meeting).

3) Access to quality feedback given by the QM team
Interpreters receive written feedback from the QM team. This feedback contains the name of the interpreter giving the feedback and will also be accessible to the Language Services Director, the Team Manager and two Interpreting and Central Support staff members responsible for interpreter administration.
In preparation for the biannual Accreditation Board meeting, members of the Accreditation Board are given access to the feedback of the interpreters concerned via a link to a folder in OpenText. Access to the folder is removed after the Accreditation Board meeting.

4) The data categories mobile phone number, e-mail address and interpreter status are made accessible to EPO interpreters on a dedicated OpenText page.

Purpose of sharing 1) Data contained in applications:
to maintain a pool of suitably qualified interpreters to provide the Office with high-quality interpreting services
2) Data shared in IAS:
for service provision
3) Data of QM feedback:
for training and quality management purposes
4) Data on OpenText: for purposes of cooperation among interpreters and training

Transfer

Transfer Yes

Country where data might be transferred - Processor (Vendors)

Transfer to public authority and/or International Organisation	**Reasons for the transfer** The Unified Patent Court (UPC) periodically asks Language Services for the names and contact details of EPO-accredited interpreters so that it can contact them with a view to engaging them. Patent law firms also occasionally ask Language Services to recommend EPO-accredited interpreters. Subject to the interpreter's consent, personal data are shared with the UPC and patent law firms. The interpreters concerned give their consent once via a consent form in MS Forms. Their response is kept in an Excel spreadsheet on Epocloud-my.SharePoint. Categories of data subjects and Categories of personal data Categories of data subjects: EPO-accredited interpreters Categories of personal data: Full name - languages - email address Purpose of sharing The purpose of the data transfer is co-operation and sharing based on the interpreter's consent., Service provider processing data only for Operations/Maintenance purposes
Transfer mechanism(s) The recipient provided appropriate safeguards	**Derogations Art. 10 DPR**

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, All personal data related to IAS are stored in secure IT applications according to the security standards of EPO. These include: • User authentication: internal access (by D444) is based on Windows authentication, with Single Sign On, based on active directory groups. External access by interpreters is made via IAS External. IAS External is defined as an Azure application (https://onpremiseiasexternal-epocloud.msappproxy.net/). Authentication is based on the Standard authentication method defined for all EPO Azure applications (Windows user account + password + Multiple-factor authentication); • Access control: IAS and IAS External have only two roles: internal users or interpreters. These roles are "hard-coded" in the application and managed by Active directory groups. Requesters are not defined in the application: any EPO user can access the public page of IAS External to submit a request for interpreters. • Physical protection: EPO access controls, additional access controls to datacentre, policies to lock offices; • Transmission and input controls (e.g. audit logging, systems and network monitoring): security monitoring with Splunk; • Security incidence response: 24/7 monitoring for incidents, on-call security expert., EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 250

Name Convergence of practice (SP2023 Programme 4.4.2)

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG5 - 52 - Legal Affairs

External processors

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

Zoom

External processors	
Name Zoom	

OpenText

External processors	
Name OpenText	

Microsoft

External processors	
Name Microsoft	

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

Zoom

External processors	
Name Zoom	

Microsoft

External processors	
Name Microsoft	

Description of the processing

Description As part of the SP2023, a Convergence of Practice Programme has been established to identify, reduce and overcome diverging practices before national patent offices and the EPO.
Each EPC Member State and extension states, the Institute of professional representatives (epi) and Business Europe are asked to submit a representative to participate in meetings and share opinions of the entity they are representing on discussed proposals. The details are collected by email and used to establish lists of participants.
The list of participants, and any e-mails sent to the participants of the working group by the Chair will possibly be stored in Microsoft tools (e.g. outlook, window explorer) or in the Case Management System of Legal Affairs (CMS). The minutes and reports will include the abbreviations of the represented States and user organisations but no indication who represented the State.
The meetings are usually held virtually and include the nominated participants of the working group from the EPC contracting states, possibly extension states, user organisations (usually epi & BusinessEurope), and the representatives of the EPO (Lawyers from the delegated controller's unit and examiners from DG1).

Data Retention There is no personal data included in the Minutes and Reports.

Personal data processed in email correspondence as well as the list of participants are kept for the default retention period of the delegated controller which is 20 years.

Purpose of Processing The co-operation programme on the convergence of practice aims at reducing or possibly overcoming these differences by setting best practices in identified areas where it could be expected that a more uniform approach would provide the most beneficial results for users and patent offices. This implementation requires the identification of the individuals representing the States or associations which participate in the discussions organised by the EPO, setting up of corresponding lists, organisation and holding of meetings, sharing opinions on the document to be prepared etc. Personal data is processed: To identify participants, to facilitate the necessary exchanges of views between the stakeholders involved, to elaborate a common proposal to be adopted by the Administrative Council of the EPO, and to keep track of the elaboration process, for historical and legal certainty purposes

Data subjects and categories of personal data

Employees

Matter/Log file	
Attachments	Metadata
General	

Any other information	Assessment and legal opinions
Input provided during the deliberation and decision-making process	
Contact Information	
Mobile Phone Number	Phone Numbers
Working email address	
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Personal information provided voluntarily	
Employment Information	
Assessment and legal opinions	Department name and/or number
Job Title Role	
Personal Identification	
Full Name	

Externals

Matter/Log file	
Attachments	Metadata
General	
Any other information	Input provided during the deliberation and decision-making process
Legal opinions and assessments	User association
Ticketing	
Ticket related data	
Contact Information	
Contact Details	Working email address
Professional Experience & Affiliations	
CV	
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information

Personal information provided voluntarily	
Employment Information	
Business Unit Division	Company Entity
Personal Identification	
Full Name	

Recipient of the personal data

Recipients of the data The participants of the working group
Senior Management of the EPO
Other units of the EPO as necessary
External Contractors involved in providing a platform for the working group

Purpose of sharing The participants of the working group are informed of the list of participants to facilitate discussions between participants (including both internal EPO employees and external participants.
Senior management of the EPO and other units of the EPO are informed of the list of be aware of who is participating, participants to monitor developments in the meetings and any conclusions drawn.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation National Patent Offices of EPC Extension States

Transfer mechanism(s) The recipient provided appropriate safeguards, Derogation in accordance with Art. 10 DPR

Country where data might be transferred - Processor (Vendors) Microsoft - United States, Zoom - United States, TRE Thomson Reuters - Luxembourg, OpenText - United Kingdom

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, International cooperation activities

Derogations Art. 10 DPR The transfer is necessary for the performance of a task in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning, or to perform obligations arising from its duty of co-operation with the contracting states

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 251

Name General Authorisations maintenance

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG5 - 53 - Patent Law and Procedures

External processors

ServiceNow

External processors	
Name ServiceNow	

Microsoft

External processors	
Name Microsoft	

Microsoft

External processors	
Name Microsoft	

ServiceNow

External processors

Name
ServiceNow

Description of the processing

Description The representation in proceedings with the EPO may be undertaken by a person registered on the list of professional representatives before the EPO, legal practitioners (Article 134(8) EPC as well as, under specific conditions, by an employee of a party (Article 133(3) EPC).

Whereas legal practitioners and employees must always file an authorisation, professional representatives are only obliged to file an authorisation in specific cases (cf. Decision of the President of the European Patent Office dated 12 July 2007 on the filing of authorisations (OJ EPO 2007, Special edition No. 3, 128). To this end, all these representatives may be individually or generally authorised (cf. Rule 152(5) EPC). General authorisations are registered, administered and deleted by the Legal Division competent to this end (OJ EPO 2013, 600).

General Authorisations must be filed in the original and are received by post or electronically via permitted OLF (online filing).

For the registration of a general authorisation the requestor(s) must provide personal data like name and address of the authorisor(s) and authorisee(s) as well as position within the company (if applicable) of the signatory.

Specific documents might be required, such as certification of employment or commercial register extract.

In case of an employee under Article 133(3) EPC, the confirmation letter
is sent to the authorisor rather than the authorised employee. In all other cases,
the confirmation letter is sent to the representative with a copy of the newly registered GA or a copy of the updated GA.

The general authorisation, including the level of rights awarded, is registered in the EPO's internal database

Data Retention Personal data processed are stored for the period of time necessary to achieve the purpose for which they have been processed.

Should a GA (General Authorisation) be withdrawn, its status would become inactive in the system. The retention time is 99 years after the withdrawal.
When a function/mandate as authorisor or authorisee is withdrawn from a running GA, corresponding status of that data subject becomes inactive. Relevant personal data is destroyed when the GA reaches the end of its retention time.

A GA and related functions of authorisor or authorisee, together with related personal data, are destroyed at the latest 99 years after the last authorisee has been withdrawn from the list in which they were registered (e.g. as professional representative, legal practitioner etc).

Purpose of Processing Registration, deletion and administration of general authorisations as well as provision of up-to-date information to internal units to ensure a proper and efficient information flow and management of associated activities in the patent grant process as well as the preparation of statistics

Data subjects and categories of personal data

Externals

Ticketing

Ticket related data	
Contact Information	
Contact Details	Country
Home Address	Phone Numbers
Working email address	
Representation in EPO's Patent Granting Process	
Affiliation to Association of professional representatives	Authorisee function
Authorisor function	EPO CDS (Client Data System) categories related to the Representation role
Representative registration number (ID)	Role in the Patent Grant Procedure
Supporting documentation	
Employment Information	
Company Entity	Job Title Role
Personal Identification	
Full Name	Gender
Surname	Signature

Employees

Ticketing	
Ticket related data	
Contact Information	
Phone Numbers	Working email address
Employment Information	
Business Unit Division	Job Title Role
Office Location	Personnel Number
Personal Identification	
Full Name	Gender

Recipient of the personal data

Recipients of the data Different business units at the EPO will have access to the information stored on the contact details database:

• DG0, DG1, DG5
• Other involvements are possible, e.g. Board of Appeals on a need-to-know basis

Purpose of sharing • DG1 as needed for the patent if required in specific patent applications.
• Other internal contact detail exports or statistics on request for DG0, DG1, DG5, on a need to know basis
• Other involvements are possible, e.g. Board of Appeals in case of an appeal

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors) Microsoft - United States, ServiceNow - Netherlands

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 252

Name Programme 4.5.3 “Improving the quality of PCT products and services”

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG0 - 02 - Communication

Entity Name - Controller (Entities) DG5 - 53 - Patent Law and Procedures

External processors

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

OpenText

External processors	
Name OpenText	

Zoom

External processors	
Name Zoom	

OpenText

External processors

Name
OpenText

Microsoft

External processors
Name
Microsoft

TRE Thomson Reuters

External processors
Name
TRE Thomson Reuters

Microsoft

External processors
Name
Microsoft

Zoom

External processors
Name
Zoom

Description of the processing

Description Programme 4.5.3 aims at strengthening the attractiveness of the EPO in the context of the PCT by further improving the quality of its PCT products and services. This programme covers projects and tracked activities that require cooperation with WIPO, PCT Contracting States including IP5 Offices. It is designed to enable the EPO to stay in the lead of endeavors for a global convergence of requirements and/or practices via the PCT, while at the same time ensuring that the interests of the EPO, its users and stakeholders are fulfilled.

Personal data is processed where it is necessary for the performance of the projects and tracked activities under this programme:

Collected data is stored on a shared drive of Directorate D 5.2.2 or in the Case Management System of PD52 (CMS), or, as far as older data is concerned, in paper form. In most cases, the personal data collected are of professional nature, i.e. names, Organisation, professional e-mail addresses, professional titles/roles, department names, correspondence, substantive comments, contributions.

Other personal data may also be collected where necessary for the organisation of meetings (e.g. meetings with WIPO and PCT Contracting States, meetings between IP5 Offices).

Collected data may be shared outside the EPO either within the context of the PCT procedure or for cooperation activities. In this latter case, the recipients are usually WIPO or an IP Office of a PCT Contracting State which are involved in the activity/meeting within the context of which the data was collected. For some meetings, the list of participants annexed to the summary of discussions of that meeting is included in a document published on WIPO's website.

In case of physical meetings, group pictures might be taken and be published on the EPO's intranet. The case be, further personal data might be processed, such as dietary habits or mobility needs.

Data Retention - The default retention period of 20 years of Legal Affairs will be applied as follows:
When a file having reached the retention period of 20 years is consulted by a staff member, it will be assessed and decided whether the said file should continue to be kept as-is, anonymised or destroyed. Files considered still necessary will be kept 10 more years, after which the same procedure applies again until destruction or anonymisation.
This approach will be revised once the available tools will allow for an automatic follow-up of retention times.
- The minutes of meetings, entailing the name of the Chairperson, as well as the list of participants are kept without time limitation.
- Information on dietary habits or physical mobility is deleted as soon as is it not anymore necessary, usually within 3 months after the event.

Purpose of Processing Data is processed within the context of the PCT procedure or for cooperation activities related to the PCT.

Data subjects and categories of personal data

Externals

General	
Any other information	User association
Contact Information	
Country	Phone Numbers
Working email address	

Professional Experience & Affiliations	
Affiliation	Professional Memberships
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Personal information provided voluntarily	
Employment Information	
Business Unit Division	Company Entity
Department name and/or number	Job Title Role
Personal Identification	
Full Name	Gender

Employees

General	
Any other information	Assessment and legal opinions
Input provided during the deliberation and decision-making process	
Ticketing	
Ticket related data	
Contact Information	
Phone Numbers	Working email address
Correspondence	
Any other information	
Employment Information	
Assessment and legal opinions	Business Unit Division
Department name and/or number	Job Title Role
Personal Identification	
Full Name	Gender

Recipient of the personal data

Recipients of the data Internal recipients: the EPO hierarchy and colleagues from other departments who are involved in projects/activities covered by Programme 4.5.3.
External recipients: WIPO, IP Offices of PCT Contracting States , the external processors, and, in rare cases, external persons/the public

Purpose of sharing Information or cooperation purposes

Transfer

Transfer Yes

Country where data might be transferred - Processor (Vendors) Zoom - United States, TRE Thomson Reuters - Luxembourg, Microsoft - United States, OpenText - United Kingdom

Transfer to public authority and/or International Organisation WIPO and IP Offices of PCT Contracting States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, International cooperation activities

Transfer mechanism(s) The recipient provided appropriate safeguards, EC Adequacy Decision, Legally binding and enforceable instrument between public authorities or bodies

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 254

Name EPO Academy

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 46 - CIO / BIT, DG4 - 45 - CTO / BIT, DG0 - 02 - Communication

Entity Name - Controller (Entities) DG5 - 54 - Patent Intelligence

External processors

Microsoft

External processors	
Name Microsoft	

Brevo | European Patent Office | Unknown

External processors	
Name Brevo | European Patent Office | Unknown	

Slido

External processors	
Name Slido	

Azavista | European Patent Office | Unknown

External processors

Name
Azavista | European Patent Office | Unknown

Microsoft

External processors
Name
Microsoft

Zoom

External processors
Name
Zoom

Description of the processing

Description The European Patent Academy is responsible for the organisation of some events (such as, online and onsite courses, lectures, seminars, conferences, workshops).

These events may also be streamed live and recorded and the recordings used for promotional and educational purposes.

The audio-visual material produced may be published on the EPO internal (e.g. Intranet, e-centre of the European Patent Academy or the internal EPO podcast page) and/or on external platforms (e.g. EPO website and podcast platforms) or social media (e.g YouTube, LinkedIn, Twitter, Facebook).

Although the EPO may use these social media channels to inform about and promote initiatives, this does not mean in any way that the EPO endorses them nor the way they process users' personal data.

During the events, if the audience is allowed to ask question (by using Slido or other applications as well as the chat/comment function on the channels of social media) the EPO will, when receiving your question, forward this question to the moderator, who in turn will inform the speaker/presenter with the mention of your first name only, without further personal information from the person asking the question, nor pictures or video from this person. Depending on the platform used, the attendees can choose to post their comment and/or opinions publicly or anonymously.

When data subjects register for events organised by the Academy, they can also indicate their interest for the mailing list.

For onsite and on-line events, EPO PD Communication organises the event contacting the speakers and all attendees in order to establish catering, dietary requirements and other preferences.

Data Retention The retention period depends on the purpose for which the data is stored: category:
(a) events: until after the event and then the contact details of the self subscription are kept for mailing purposes.
(b) Audio visual material originating from events, is kept for a maximum period of 25 years.

Purpose of Processing Organisation of training and conferences for external stakeholders, The carrying out of the Academy's statutory duties

Data subjects and categories of personal data

Externals

Contact Information	
Contact Details	Country
Working email address	
Professional Experience & Affiliations	
CV	
Correspondence	
Additional Information which might be provided in the course of exchanges	Personal information provided voluntarily
Employment Information	
Business Unit Division	Language preference (of communication)
Personal Identification	
Full Name	
Education & Skills	
Education and Training History	Educational Degrees
Languages	

Employees

Contact Information	
Contact Details	Country
Working email address	
Correspondence	
Personal information provided voluntarily	
Employment Information	
Department name and/or number	Language preference (of communication)
Office Location	
Personal Identification	
Full Name	
Education & Skills	
Languages	

Recipient of the personal data

Recipients of the data Recipients from operational units within the European Patent Office also recipients outside the European Patent Office such as agencies or entities performing a peer review.

Purpose of sharing The purpose is to achieve the operational result for which the data is collected, such as the organisation and smooth running of the events .

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors) Zoom - United States, Microsoft - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 255

Name European Patent Administration Certificate (EPAC)

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 41 - Finance, DG4 - 46 - CIO / BIT, DG4 - 45 - CTO / BIT

Entity Name - Controller (Entities) DG5 - 54 - Patent Intelligence

External processors

UNIwise

External processors	
Name UNIwise	

UNIwise

External processors	
Name UNIwise	

ServiceNow

External processors	
Name ServiceNow	

Description of the processing

Description Personal data is processed by the EPO to successfully organise and manage the European Patent Administration Certification and follow-up actions in accordance with the Rules concerning the establishment of a European Patent Administration Certification (EPAC) decided by the President of the EPO (pending).

The EPAC is a professional certification for patent administrators organised by the EPO. EPAC certifies the mastering of procedural administrative tasks relating to the patent granting procedures under the legal systems of the European Patent Convention (EPC) and the Patent Cooperation Treaty (PCT).

The present document aims at providing information on how the personal data are processed in the context of the different stages and activities of EPAC, such as the enrolment of the candidates, the correct performance of the certification and the review process.

The European Patent Academy is in charge of the organisation and conduct of the EPAC. It shall decide on the result of each examination upon proposal of the EPAC Board, a certification support group in the sense of article 5 of Decision CA/D 7/21 of the Administrative Council of the European Patent Organisation.

These activities include the processing of personal data for candidates' enrolment and the payment of the fees.
Candidates with disabilities are flagged in the system as needing special arrangement, the medical details of the disability as such are not named nor stored, since only compensation is offered.
Correspondence with candidate is kept in his/her file as long as the candidate is active in the EPAC.

EPAC can be done via an online platform.

The external supplier that provides the online platform process personal data on the EPO's behalf and it oversees the maintenance of the platform and offer support. The online platform has proctoring features to monitor the candidates during the examination to prevent attempts of fraudulent behaviour and keep proof of them, where deemed necessary.

Pursuant to Article 3(2) of the Rules concerning the establishment of EPAC, the EPAC Board is established for a three-year mandate and tasked with the drafting and marking of the EPAC examination. It shall make a proposal on the result of each examination to the Academy. The results are made available to each candidate.

According to Article 16 of the Rules concerning the establishment of EPAC, candidates' anonymity shall be respected when their answers are marked and their answers may be published for research, statistical or training purposes provided their anonymity is respected.

A review procedure before the EPAC review Board is possible in accordance with Articles 5 and 12 of the Rules concerning the establishment of EPAC. Candidates may request the review of a decision adversely affecting them. The request must be filed within a time limit of two weeks after notification of the decision and pay a review fee. The EPAC review board will inform the candidate of its decision in writing by electronic means. The decision of the EPAC review board is not subject to any further means of redress.

Members of the EPAC Board and EPAC review Board provide their data when becoming member of the respective body.

Purpose of Processing Administering EPAC which is a certification decided by the President within the framework of Decision CA/D 7/21 of the Administrative Council of the European Patent Organisation dated 13 October 2021 on modernising the structures of the European Patent Academy. Personal data are to be processed in order to: - decide whether the conditions to enrol are fulfilled - identify candidates - process payment - accurately associate candidates' answers, - keep previous results: if the first part has not been passed, the examination will be considered as failed and the other part(s) will not be marked. - ensure that EPAC is conducted properly (including technical support to the candidates by the EPO master users) and attempts of fraudulent behaviour are prevented or proven - process review requests - management of online candidate file - issue a certificate to successful candidates - publish a list of successful EPAC candidates as a searchable database on the website of the EPO. - select EPAC bodies members and manage their files

Data Retention Depending on the categories of personal data processed, the personal data can be kept for different periods.

Personal data processed by the data controller or the service providers under its supervision are generally stored for the period necessary to achieve the purpose for which they have been processed. This applies to all documents and information obtained and produced in electronic and/or paper form in connection with a candidates' enrolment and participation in the EPAC.

Facial images, audio and biometric data produced from webcam and audio captures, the content of the communication (chat) will be retained by the processor's and sub-processors' systems for maximum 6 months.

In a case of suspected misconduct and/or review request the data, which are mentioned above as being retained by the processor and the sub-processors for a short period, will be copied and retained by the EPO in accordance with the Retention Policy

Data subjects and categories of personal data

Employees

Learning managements metrics	
Ratings	
Contact Information	
Contact Details	Country
Mobile Phone Number	Phone Numbers
Working email address	
Biometric	
Facial Recognition	
Correspondence	
Additional Information which might be provided in the course of exchanges	Chat content
Examination content data	
Examination marks	Examination result
Online invigilation data	
Audio input	Webcam captures
Employment Information	
Language preference (of communication)	Office Location
Personal Identification	

Date of Birth	Disability or Specific Condition
Full Name	Gender
Nationality	Picture
Education & Skills	
Education and Training History	
Government Identifiers	
National Identity Card Details	Passport Number

Externals

Learning managements metrics	
Learning history	Ratings
Contact Information	
Contact Details	Country
Mobile Phone Number	Phone Numbers
Working email address	
Biometric	
Facial Recognition	
Correspondence	
Additional Information which might be provided in the course of exchanges	Chat content
Examination content data	
Examination marks	Examination result
Online invigilation data	
Audio input	Webcam captures
Employment Information	
Language preference (of communication)	
Personal Identification	
Date of Birth	Disability or Specific Condition
Full Name	Gender
Nationality	Picture

Education & Skills	
Education and Training History	Languages
Government Identifiers	
National Identity Card Details	Passport Number

Recipient of the personal data

Recipients of the data The EPAC Board and EPAC review Board have access to the data of candidates to the extent needed to perform their respective duties as defined in of the Rules concerning the establishment of EPAC.

Depending on the EPACQE body, access to the data is granted on a need-to-know basis to EPO and non-EPO staff.

According to Article 17 of the Rules concerning the establishment of EPAC, all EPO employees as well as external experts involved during and after their term of office shall be guaranteed with regard to all matters concerning EPAC and the candidates.
The personal data is disclosed, on a need-to-know basis, to the following recipients:
• the EPO's staff members of the European Patent Academy;
• members of the EPAC board and EPAC review Board;
• EPO authorised users (`master` users);
• Administrators of the WISEflow platform at UNIWise and its subprocessors (management of ticketing of incidents and to the following data of the candidates and the members of the Examination Committees for the bidirectional communication channel (chats) during the examination; hosting services);
• BIT
• Finance departments for the fee processing

Purpose of sharing Data is shared with the EPAC Board and the EPAC review Board. The purpose of sharing is the proper organisation and carrying out of the EPAC programme (examination and certification)

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards, Data Protection EU Comm Standard Contractual Clauses

Country where data might be transferred - Processor (Vendors) ServiceNow - Netherlands, UNIwise - European Union

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, Treatment of data

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums)., To mitigate the risk of a conflict of interest within the EPO (EPO employees may sit the EPAC) access to data is restricted to a very limited group of persons. Technical means protect the violation of confidentiality as far as possible, even from system administrators. Technical staff of the service providers who cannot be exempted from access are individually known and bound by a confidentiality declaration. All personal data are stored in secure IT applications according to the security standards of the EPO. External providers are under strict contractual obligation as defined by Procurement and BIT standards. Limited access to data is given to technical staff of the provider on an event driven basis for the purpose of system administration and error analysis. For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. Except for a specific purpose defined in advance by the DPS, only the minimum necessary data are shared with other external parties. These parties have systems which are in conformity with the EPO security standards and have implemented the appropriate technical and organisational measures in this respect. All members of EPAC bodies are bound by secrecy under Article 17 of the Rules concerning the establishment of EPAC. Access to these data is protected by the personal user accounts of the members. Marking of the answers is anonymous. Financial procedures for the administration of fee payment are executed by the EPO Finance department and their service providers., For the data processing by UNIWise , UNIWise concluded a DPA , incl. EU SCCs, according to BIT

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 256

Name Organisation of Meetings between Legal Affairs and EPI

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG5 - 53 - Patent Law and Procedures

External processors

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

Zoom

External processors	
Name Zoom	

Microsoft

External processors	
Name Microsoft	

Microsoft

External processors

Name
Microsoft

Zoom

External processors
Name
Zoom

Description of the processing

Description Legal Affairs (PD52) holds regular meetings with representatives of the Institute of Professional Representatives before the EPO (epi) to discuss the cooperation between the EPO and epi.

Physical (or virtual) meetings are organised on an annual basis by PD52. When a meeting is being organised, an electronic file is created in the Case Management System (CMS) of the directorate under a specific log number together with the name of the responsible lawyer.

Legal affairs will provide details of the meeting to other participating directorates of the EPO. Legal Affairs will request the necessary information (agenda points, time schedule, etc.) from participants by email, and save that information in the corresponding CMS file.

The data is used by the EPO to organise the meeting and communicate related information to the participants or, on a need to know basis, to other stakeholders including:
*Technical aspects to be dealt with for the meeting itself (e.g. digital platform).
*Exchanges prior to the meeting e.g. preparation of the agenda, documents to be prepared and discussed.
*Exchanges after the meeting including sharing minutes, documents, possible follow-up actions.

The correspondence and documents exchanged before, during and after the meeting are saved in the CMS file. The Minutes of the meeting are then distributed to all participants of the meeting by email.

If applicable, notes or reports will be created after the meeting, including the name of the attendees, position and organisation represented, and distributed to the Hierarchy. In addition, documentation organising the meeting are stored on EPO Shared-Drive (W: drive) and CMS.

The active processing of personal data (mostly exchange of emails) stops after the end of possible follow-up actions/exchanges taking place after the meeting.

Data Retention Personal data necessary for organising meetings are kept until the next meeting has been organised.
The list of attendees and non-anonymised minutes are kept 10 years after the meeting.

Purpose of Processing Meetings between the Legal Division/EPO and epi are organised to discuss the collaboration between the Legal Division and epi. Personal data is processed to organise and facilitate the meetings, record the key conclusions of the meeting in the form of minutes, notes or reports (if applicable) and to distribute these conclusions to participants and the EPO hierarchy.

Data subjects and categories of personal data

Employees

General

Any other information	
Contact Information	
Phone Numbers	Working email address
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Personal information provided voluntarily	
Employment Information	
Department name and/or number	Job Title Role
Personal Identification	
Full Name	Gender

Externals

General	
Any other information	
Contact Information	
Phone Numbers	Working email address
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Personal information provided voluntarily	
Employment Information	
Company Entity	Department name and/or number
Job Title Role	Language preference (of communication)
Office Location	
Personal Identification	
Digital signature	Full Name
Gender	

Recipient of the personal data

Recipients of the data Internal and external participants of the meeting.
Hierarchy of the EPO.
External processors.

Purpose of sharing Internal and external participants receive the minutes of the meeting, and any other personal data that is shared in the organisation of the meeting.
Hierarchy of the EPO receives minutes and if applicable notes or reports summarising the key conclusions from the meeting.

Transfer

Transfer Yes

Country where data might be transferred - Processor (Vendors) TRE Thomson Reuters - Luxembourg, Zoom - United States, Microsoft - United States

Transfer to public authority and/or International Organisation

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Transfer mechanism(s) The recipient provided appropriate safeguards

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 268

Name Personal data processing in editing/translation services-DG4 - PD44 - General Administration | European Patent Office | Germany

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 44 - General Administration

Entity Name - Controller (Entities) DG4 - 44 - General Administration

External processors

Microsoft

External processors	
Name Microsoft	

CBG

External processors	
Name CBG	

Acolad

External processors	
Name Acolad	

RWS (SDL)

External processors

Name
RWS (SDL)

Microsoft

External processors
Name
Microsoft

Description of the processing

Description The present processing of activities concerns the editing and translation work done in Translation and Editing.
Editing and/or translation requests are submitted by EPO staff or any EPO department via the request form in WorldServer (WS) on the Language Services' Intranet site.
After submission of a request, the following steps happen:
1) Documents of the request are uploaded on the WorldServer (WS) server.
2) WS creates the folder structure for the request on Byblos and copies the document(s) in the source folder.
3) WS creates the request in the database
4) The documents submitted with the request are then edited and/or translated in Translation and Editing or outsourced.
5) Part of the documents submitted to Translation and Editing are also formatted by the document design unit in Language Services/Interpreting Services and Central Support before and/or after editing/translation.
6) In the case of outsourcing editing/translation work in the official languages to the contractor CBG, assignments to edit or translate the documents are made available on the WorldServer portal of the EPO, and the contractor is informed that new assignments are available through email notifications.
Delivery from the contractor to D Language Services is made when the completed assignment is uploaded on the WorldServer portal or exceptionally transmitted per email to D Language Services if the portal is temporarily unavailable.
7) During outsourcing, personal data will be processed by the contractor, who will also be working with sub-processors. Additionally, the contractor CBG will act as the interface between the EPO and designated specialists for assignments requiring specific expertise (Project management of "specialist assignments"). Specialist assignments are only used for specific documents (patent law). This does not encompass the activities undertaken for distribution of work inside the Language Service. The designated specialists do not include CBG's employees. All specialists are subprocessors of CBG.
8) The workflows for outsourcing editing/translation work in the non-official languages are currently being adapted
9) During the editing/translation process the original as well as the edited/translated versions of the document are stored on Byblos, in WorldServer (translation memories) and in MultiTrans (text corpora), which are systems servers on EPO premises (EPO Data Centre LUX).

10) After completion of the requested service, edited and/or translated texts which have not been stored automatically during the processing, mainly because they could not be treated with the CAT-tool (Computer Assisted Translation) for technical reasons, are aligned manually for the purpose of updating the Language Service's translation memories (WorldServer) and text corpora (MultiTrans). This is done by Translation and Editing and will soon be overtaken partly by the external contractor CBG.
11) After completion of the requested editing/translation, a link to Byblos is sent via email (Outlook mailbox of the individual editor/translator responsible for the request). This is the standard procedure with respect to requesters who are staff members of D Council Secretariat and for delivering edited and/or translated confidential documents. If the requesters are other EPO employees and the edited and/or translated document is non-confidential, it is attached to the email sent by the respective editor/translator.
Processing is partially automated.

Data Retention For documents stored in OpenText, the retention time is 15 years.
Retention time on WorldServer and MultiTrans still to be defined.
No data are stored in Machine translation.

Purpose of Processing Personal data is processed in the context of delivering the requested editing/translation services. The processing of personal data during editing/translation can in some cases be necessary for linguistic reasons (e.g. in some languages, pronouns are gender specific). The storage of edited/translated documents serves the purpose of quality, efficiency and knowledge management, e.g. in order to reuse edited/translated texts for future requests, or to keep editings/translations revised/done by senior colleagues as a reference for knowledge management. -> This process of storing edited/translated documents and the corresponding source files including any personal data contained therein is currently under review with a view of implementing an anonymization process. Legal basis for editing/translating documents including eventual personal data contained therein: Article 14 (1), 31 EPC Article 14 EPC: "Languages of the European Patent Office, European patent applications and other documents" Article 31 EPC: "Languages of the Administrative Council _____
For the purpose of providing a remote hosted machine translation service to 4.4.3.1 staff, the company RWS processes personal data of EPO staff in 4.4.3.1 who can use the remote hosted machine translation service via their Computer Aided Translation (CAT)-Tool which is available to them under a licence.
_____ Purpose of storing pictures taken of former and current 4.4.3 staff members at team events: fostering team spirit and for collective memory

Data subjects and categories of personal data

Employees

Health Data	
Health Data	
Contact Information	
Phone Numbers	Working email address
Professional Experience & Affiliations	
CV	Trade Union Membership
Employment Information	
Appeals Records Information	Disciplinary Action
Duration of employment	Grade
Job Group	Job Title Role
Membership in a EPO Staff Committee	Performance Rating
Rewards history	
Personal Identification	
Date of Birth	Full Name
Nationality	
Education & Skills	
Education and Training History	Languages

Prospective Employees

Contact Information	
Contact Details	Home Address
Phone Numbers	Working email address
Professional Experience & Affiliations	
CV	
Employment Information	
Performance Rating	
Personal Identification	
Date of Birth	Full Name
Nationality	

Education & Skills	
Education and Training History	Educational Degrees
Languages	

Externals

Health Data	
Health Data	
Contact Information	
Personal Email	Phone Numbers
Working email address	
Professional Experience & Affiliations	
CV	
Personal Identification	
Date of Birth	Full Name
Nationality	
Education & Skills	
Education and Training History	Languages

Recipient of the personal data

Recipients of the data Personal data contained in documents sent to Language Services for editing/translation is accessible only to EPO staff members within Translation and Editing and Interpreting Services and Central Support and, in the case of outsourcing, to external contractors.

Purpose of sharing Only to service provider to perform the service.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors) Microsoft - United States

Reasons for the transfer Service provider sub-processing the data to deliver the service. This is covered in the DPA.

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums)., All personal data related to [Personal data processing in the area of editing/translation (Editing and Translation)] are stored in secure IT applications according to the security standards of EPO. These include: • User authentication: Windows authentication for all applications. WorldServer and MultiTrans have Single Sign On (SSO), so the user does not have to enter his Windows username and password manually. Byblos supports SSO. User authentication is based on Active Directory Groups, managed via MIM. This authentication method applies for all three applications (WorldServer, MultiTrans and Byblos). External vendors can access WorldServer via an azure app which supports SSO for external users. • Access control in WorldServer is based on user types, which correspond to roles (Translation and Editing + Interpreting and Central Support or vendor or requester). These are maintained within the WorldServer application. For Byblos, standard ACL groups provided by Byblos are used. In MultiTrans, access control is managed within the application and is limited to two roles: admin or regular user. • Logical security hardening of systems, equipment and network: 802.1x for network access, encryption of endpoint devices, AV on all devices • Physical protection: EPO access controls, additional access controls to datacentre, policies to lock offices; • Transmission and input controls (e.g. audit logging, systems and network monitoring): security monitoring with Splunk; • Security incidence response: 24/7 monitoring for incidents, on-call security expert. For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment (PSRA) has been carried out by the EPO. The contractors CBG and Acolad filled in the standard questionnaire.

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 269

Name Document design services

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 46 - CIO / BIT, DG4 - 44 - General Administration

Entity Name - Controller (Entities) DG4 - 44 - General Administration

External processors

Softserve

External processors	
Name Softserve	

Paragon

External processors	
Name Paragon	

PresentNow

External processors	
Name PresentNow	

Global Lingo

External processors

Name	
Global Lingo	

Description of the processing

Description 1) Personal data are collected in the context of processing of requests for document design work (such as transcriptions of witness hearings in oral proceedings, the formatting of documents, the creation of templates) are submitted by EPO staff via ServiceNow.
2) The Document Design Team receives these requests in ServiceNow under a ticket number as a link.
3) The requests are then processed internally or outsourced (transcriptions are always outsourced). In the case of outsourcing, personal data is sent via a generic Outlook mailbox (Document Design) to the external contractors, who return work via the same mailbox. An exception is the outsourcing of transcription requests to the external provider Global Lingo, for which Document Design uses the company's GloZone portal. Global Lingo returns the completed transcriptions via the generic Outlook mailbox Document Design.
4) During the transcription/document design process, data (i.e. audio files, transcriptions as well as original and newly formatted files) are stored in ServiceNow under the ticket number. In the case of requests submitted by Translation/Editing (concerning the formatting of documents), original and newly formatted files are also stored on Byblos.*

5) After completion of work, the transcriptions/formatted documents are sent back (as an attachment) to the requester via ServiceNow; requesters from Translation/Editing receive an email with a link to Byblos where the formatted documents and their original versions are stored.
Processing is partially automated.
* the requests/tickets are stored in ServiceNow and the link to the file on Byblos is/remains available in the request/ticket.

Data Retention Transcription via ServiceNow: 1 year
All other requests/tickets: 5 years

Purpose of Processing Personal data contained in transcriptions and documents received for formatting is processed in the context of delivering the requested document design services.

Data subjects and categories of personal data

Employees

Health Data	
Health Data	
Contact Information	
Contact Details	Phone Numbers
Working email address	
Professional Experience & Affiliations	
CV	Trade Union Membership
Employment Information	
Company Entity	Job Title Role
Membership in a EPO Staff Committee	Performance Rating

Previous Work History	
Personal Identification	
Full Name	Nationality
Education & Skills	
Education and Training History	

Externals

Health Data	
Health Data	
Contact Information	
Contact Details	Phone Numbers
Working email address	
Professional Experience & Affiliations	
CV	
Employment Information	
Company Entity	Job Title Role
Previous Work History	
Personal Identification	
Full Name	Nationality
Education & Skills	
Education and Training History	

Recipient of the personal data

Recipients of the data The personal data contained in audio files, the requested transcriptions and in documents sent for formatting is accessible only to the Document Design staff responsible for transcriptions and document design.

In the case of outsourcing, the personal data mentioned above is also accessible to external contractors.

In the case of formatting requests relating to documents which are edited and/or translated after/before formatting, the documents concerned are also accessible to the editors/translators in Document Design as well as to external editors/translators in the case of outsourcing.

As for audio files/transcriptions/documents stored in ServiceNow, the tickets are accessible only to the Language Services staff members responsible for transcriptions and document design and the application manager.

Purpose of sharing To deliver the requested document design services.

Transfer

Transfer No

Country where data might be transferred - Processor (Vendors)
Global Lingo - United Kingdom

Transfer to public authority and/or International Organisation

Reasons for the transfer

Transfer mechanism(s)

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 274

Name Invoicing

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 45 - CTO / BIT

Entity Name - Controller (Entities) DG4 - 41 - Finance

External processors

Jouve SAS

External processors	
Name Jouve SAS	

Description of the processing

Description 1. Invoices arrive via a common mail address as .pdf attachments to emails in the EPO mail rooms.
2. The mailroom staff uploads the PDF invoices in iValua Invoice Data Capture. This tool convert the PDF via optical character recognition (OCR) from a pure image into an e-invoice readable for SAP (IDOC). Mailroom staff checks and corrects the result of the OCR conversion if needed.
3. The IDOCs plus the image are then sent into SAP VIM, a SAP solution for vendor invoice management.
4. In VIM, the actual invoice processing is taking place fully automated i.e. the automatic booking, formal compliance check, duplicate check and matching with the goods/service receipt by the responsible budget holder.
5. In case of exceptions, the automatic processing stops, and VIM creates an error message specific to the exception.
6. If all steps under No.4 and No. 5 are completed the respective invoice is ready for payment when becoming due.
The invoicing process in the scope of this record comprises the steps No. 4 and 5

Reimbursements to staff and reimbursements to externals follow a similar process except for points 1 and 2 which are as follows:
1. Reimbursements requests are submitted via ad-hoc portals, e.g. the Single Access Portal
2. Reimbursements requests from staff are subject to a pre-check by HR staff and are then sent to SAP VIM. Reimbursement requests from externals are directly sent to SAP VIM.

Purpose of Processing Verification of invoices assuring correct and timely payments

Data Retention 12 years

Data subjects and categories of personal data

Externals

Contact Information	
Country	Home Address
Personal Email	Working email address
Financial	
Bank Account Information	Bank Account Number
Bank details	Fund Reservation Requests
Travel & Expense	
Expense Details	
Employment Information	
Hours of Work	
Personal Identification	
First Name	Surname

Prospective Employees

Contact Information	
Country	Home Address
Financial	
Bank details	
Travel & Expense	
Expense Details	
Employment Information	
Job Application Details	
Personal Identification	
First Name	Surname

Contractors

Financial	
Fund Reservation Requests	
Travel & Expense	
Expense Details	
Employment Information	
Department name and/or number	Personnel Number
Personal Identification	
First Name	Surname

Employees

Contact Information	
Working email address	
Financial	
Fund Reservation Requests	
Travel & Expense	
Expense Details	
Employment Information	
Department name and/or number	Personnel Number
Personal Identification	

First Name	Surname

Recipient of the personal data

Recipients of the data EPO Budget Holders/SIG 3, exceptionally Procurement Officers, very exceptionally with suppliers

Purpose of sharing Budget Holders/SIG 3 need to confirm the correctness of invoices thus it's often needed to share information disclosed on invoices with them.
Exceptionally, invoices are shared with Procurement Officers to clarify deemed differences in pricing and other contractual issues (EDP, VAT, payment terms etc.). The same applies for suppliers issuing the respective invoice.

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 277

Name Data Protection Board - Case management for complaints lodged by external data subjects

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 44 - General Administration

Entity Name - Controller (Entities) DG5 - 52 - Legal Affairs

External processors

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

Microsoft

External processors	
Name Microsoft	

OpenText

External processors	
Name OpenText	

Microsoft

External processors

Name
Microsoft

Description of the processing

Description As part of the means of redress available to data subjects, a complaint may be filed with the Data Protection Board against a decision by a delegated controller rejecting a request for review (Article 50 of the Data Protection Rules). Upon receipt of a complaint, the Data Protection Board notifies the delegated controller author of the review decision. When complainants are not EPO staff members, the delegated controller liaises with PD52. PD52 provides in-house case-management and legal services and arrange the mandating of an external law firm to defend the position of the delegated controller in the proceedings.

This includes:
- arranging assistance and/or representation by an external law firm
- organising and maintaining the case file
- collecting relevant facts and evidence, analysing and advising on the case
- liaising with the delegated controller at stake
- preparing and/or checking submissions to be submitted to the Data Protection Board
- assisting in alternative dispute resolution attempts.

For this activity, personal data of the persons directly or indirectly involved in a complaint are processed, partly by automated means.

Information related to a case, including personal data, are collected via pleadings and evidence submitted from the parties to proceedings, third parties (e.g. witnesses), publicly available sources (e.g. internet searches), or
gathered from other Office's units in the course of fact-finding activities when preparing a case (e.g. delegated controller at stake, BIT...).

The personal data collected can be about the parties or others. The categories of personal data processed depends on the subject matter of a case and may occasionally include special categories of data.

Information related to a case is stored electronically in a document management system and in the electronic files kept by Legal Affairs. In some cases, a paper file is created.

Information related to a case are used in documents produced along the proceedings and exchanged between the parties or submitted to consultative (Data Protection Board) and decision-making (controller) bodies.

Information related to a case is shared within the Office as necessary for example to allow verification of factual elements, to inform or consult other services, to request translation, or in the course of approval or reporting process.

Information related to a case is transmitted outside the Office as necessary, for example when an external law firm is involved.

References to cases are included in lists kept for monitoring case statuses, for reporting and for statistical purposes.

Purpose of Processing Personal data is processed for the purpose of the EPO's administrative functioning, here in particular: 1- for assisting and/or advising and/or representing the delegated controller in the proceedings before the Data Protection Board 2- enabling the availability of complaint files for later reference in the event of subsequent litigation 3 – for archiving and statistical purposes.

Data Retention In the absence of a specific reason to retain a file:

Cases that proceeded to resolution by arbitration :
* 10 years after the arbitrator's final decision was pronounced, the parts of the file relating to the precedent stages of litigation are destroyed.
* 15 years after the arbitrator's final decision was pronounced, all parts are destroyed.

Other cases:
* 10 years after the closing of the complaint stage by withdrawal, unchallenged final decision or amicable settlement, all parts of the file other than the Data Protection Board's opinion and the final decision on the complaint are destroyed.
* 15 years after the closing of the complaint stage by withdrawal, unchallenged final decision or amicable settlement, all parts are destroyed.

This applies to both electronic and paper files.

An index of cases with limited personal data categories (reference, name, status) is kept indefinitely.

Data subjects and categories of personal data

Externals

Applications' Log	
SAP Logs	
Social	
Social Media Account	Social Media Contact
Sensory and Electronic Information	
Audio Information	Electronic Information
Presence Status	Time stamps from their access to the buildings
Visual Information	
Building area and site	
Building area and site	
Representation in EPO's Patent Granting Process	
Affiliation to Association of professional representatives	All data provided upon request for entry or change
Authorisee function	Authorisor function
EPO CDS (Client Data System) categories related to the Representation role	Representative registration number (ID)
Role in the Patent Grant Procedure	Supporting documentation
Telephony Interaction Data	

Telephony Session Content	Telephony Session Details
Telephony Session Metadata	
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name
Gender	Surname
Nationality	Picture
Signature	
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
Project management experience	
Matter/Log file	
Attachments	Metadata
General	
Answers to surveys, assessments or quizzes	Any other information
Input provided during the deliberation and decision-making process	Legal opinions and assessments
Nomination justificative	User association
Contact Information	
Contact Details	Country
Emergency Contact Details	Home Address
Mobile Phone Number	Personal Email
Phone Numbers	Private Phone Number

Working email address	
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
IDP	Instructor related data
Learning external events	Learning history
Learning plan	Ratings
Social learning inputs	
European Patent Register Data	
Address	Data provided by the data subjects
Device Management Data	
Account ID	AppleID for iOS/iPadOS Devices
Azure Active Directory Device ID	EAS Device ID
Encryption Keys	Intune Device ID
Intune Device Management ID	Last Logon Time
MAC Address	Managed Application Device Tag
Managed Application ID	Platform-specific IDs
Tenant ID	Windows ID for Windows Devices
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of a patent (claims, description, drawings, abstract)
Personal data potentially included within the content of patent procedure related information and publications	
System Logs	
Audit Logs (a.k.a. Audit Trail)	File data (name, size and/or hash)
Firewall/Router/Switch Logs	Ports

Registry data	Running Processes
System-, Application-, Security-related Server Logs	Transaction-related Details
Web Servers Logs	
Phone Call Information	
Called Phone Number	Caller's Phone Number
Phone Call Date and/or Time	Phone Call Duration
Phone Call Interaction History	Phone Calling History
Ticketing	
Ticket related data	
Physical and/or Digital Identifiable Assets	
Digital Certificate	ICCID (Integrated Circuit Card Identification Number)
IMEI Number (International Mobile Equipment Identity)	Mobile Device Name
Mobile Device Serial Number	Mobile Device's Network Adapter MAC Adress
Operating System Version	Smart Card Number
Videoconference Room/Equipment Identifier	Workstation Serial Number
Workstation's Hostname (Physical or Virtual)	Workstation's Network Adapter MAC address
Biometric	
Facial Recognition	Voice Recognition
Online invigilation data	
Audio input	Webcam captures
Employment Information	
Active/Inactive Indicator	Business Unit Division
Company Entity	Contract Type
Corporate Credit or Debit Card Numbers	Department name and/or number
Duration of employment	End Date
EPO access badge number	Hours of Work
Job Title Role	Language preference (of communication)

Membership in a EPO Staff Committee	Office Location
Previous Work History	Record of Maternity Leave
Unknown	
EPO badge validity	Identification of which membership is envisaged
Price list for discounts	
Network/application Interaction Data	
Session content	Session details
Session metadata	
Health Data	
Dietary requirements	Health Data
Mobility needs	
Professional Experience & Affiliations	
Affiliation	CV
Entry or deletion date as member of an association	Political Affiliation and Activities
Professional Memberships	Qualifications Certifications
Examination content data	
Examination marks	Examination result
Financial	
Bank Account Information	Bank Account Number
Bank details	Credit Card Number
Debit Card Number	Fund Reservation Requests
Information on home loans	Insurance Information
Browsing Information	
Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
Category	Cookie Information
IP Address	Network Interaction History

URL	Website History
User Account Information	
Account Age	Account Number
Account Password	Membership Permissions
Ownership Permissions	Password Hash
Third-party User Identifier	User ID
Government Identifiers	
ID/Passport picture	National Identity Card Details
Passport Number	

Employees

General	
Assessment and legal opinions	Legal opinions and assessments
Contact Information	
Contact Details	Working email address
Employment Information	
Assessment and legal opinions	
Personal Identification	
Full Name	Gender

Recipient of the personal data

Recipients of the data Personal data can be included in diverse communications or legal documents sent :
- to other operational units (such as delegated controller author of the review decision, Employment Law, Language Services...depending on the case, also to hierarchical line (VP5 assisted by CILO and President of the Office);
- to the Data Protection Board;
- possibly to external attorneys.

Purpose of sharing - to other operational units or staff members (such as delegated controller author of the review decision, Employment Law...): for fact-finding purposes, information and/or consultation on a strict need-to-know basis.
- Language Services: for obtaining a translation.
- Depending on the case at hand, personal data can be shared with the hierarchical line (VP5 assisted by CILO and President of the Office), for ex. for approval process and reporting purposes.
- to the Data Protection Board: for the conduct of the proceedings.
- possibly to external attorneys: for the conduct of the proceedings.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation N.a.

Country where data might be transferred - Processor (Vendors) TRE Thomson Reuters - Luxembourg, OpenText - United Kingdom, Microsoft - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Transfer mechanism(s)	Derogations Art. 10 DPR
The recipient provided appropriate safeguards	

Organisational and security measures

Organisational and security measures
EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 281

Name Personal Data processing performed within the Logistic Centre activities - officewide -DG4 - PD 44 - General Administration

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 44 - General Administration

Entity Name - Controller (Entities) DG4 - 44 - General Administration

External processors

Transport/drivers companies

External processors	
Name Transport/drivers companies	

Microsoft

External processors	
Name Microsoft	

Shipping companies

External processors	
Name Shipping companies	

Courrier companies

External processors

Name
Courrier companies

Description of the processing

Description The Logistics Centre is responsible for several activities within the EPO. The services requiring personal data collection, processing and storage are as follow:

1. Drivers / Transport
The requests are received by email, phone and the data subject must share email address, name, pick-up and drop-off location, timing for trip and mobile number. For a given trip, the driver details are also requested and stored.
In The Hague, the personal data are stored in SharePoint in the driver logbook.
In Munich, the personal data are stored in the Outlook inbox and deleted after the invoicing (between 1 to 8 weeks).

2. Printing Queue / Software- Patent related

The formalities officer's and/or examiners request print work to be done using one of the patent tools which automatically get transferred to the software. From this software the requests are sent to the printers by one staff of the Logistics Centre.
The request contains personal data of the requester (Staff ID) and some personal data are contained in the document to be printed.
In The Hague, external contractors proceed with the printing work, whereas in Munich, the work is carried out by internal and external staff.
A back-up of the printing works is kept in the EPO Database. The data about printing are kept in order to prepare top management dashboard and/or in case of investigation.

3. Printing / Copying

3.1 Paper dashboard
A Paper Consumption Dashboard, created with Tableau, monitors the Office's paper usage, offering personalised statistics to promote awareness of copying's and printing's environmental impact. Employees can compare their behaviour to the office average, fostering positive changes. The Dashboard, ensuring privacy, allows only individual access to personal data for efficient tracking of resource and paper consumption. The smallest accessible level of analysis is the team level, with a minimum of 8 employees, accessible to both employees and the dashboard team.

The following personal data are collected for this purpose:
· user ID
· organisational assignment (department, area, team and/or service)
· print job ID

This aggregated data will be accessible to:
- Department BIT-Business Analytics CoE and staff working on the dashboard, for the administration of the Tableau tool, and managing data and follow-up
- the respective staff member, for observing and tracking their own and their team's printing behaviour.

Personal data is not used for any other purposes or disclosed to any other recipient(s).

3.2 Printing - other
Any staff within the EPO can request any work-related printing by email. The name, email address, phone number, office location are required. Office-wide, once the work is delivered, the email is deleted in Outlook.

Purpose of Processing The Logistics Centre needs to process personal data in connection with their daily activities and services delivery such as courier, printing, transport, office supplies… The data is registered to comply with some of the requirements established under several ISO standards on which the Office is certified (e.g. PDCA improvement cycles of ISO 9001, 45001, 27001) as well as the follow up of risk logs that are part of those ones (e.g. ISO 45001).

4. Incoming Mail and parcels
Airbills is the tool registering all the incoming parcels and envelops that require signature from the recipient. The envelops or packages are scanned and the data transferred in Airbills containing the sender and recipient addresses, names, signatures.

5. Outgoing Mail and parcels
Regmail is the tool for outgoing registered parcels and envelops. The envelops or packages are scanned, and the data transferred in Regmail containing the recipient address and name. The courier service internet application is also used to ship parcels. The recipient address, email, phone number are entered to proceed with shipment.

6. Office supply
Office wide, stationaries are requested via EPO intranet stationary portal (https://epoprod.service-now.com/sp?id=sc_category&sys_id=b94030b71ba785d05b05c9936b4bcba3&catalog_id=-1).

The EPO staff select items for the order to be delivered and submit the request. The logistic center receives an automatic email containing: the name, the location, the phone number, and the content of the order. Once the delivery is done the request and related information are deleted.

Data Retention 1. Driver/Transport
The requests and associated personal data of the EPO staff are kept until the service is performed and invoice is received by the EPO, maximum 8 weeks.
The personal data of the driver are kept for 1 year (in case of litigation, fines….).

2. Printing queue/software- patent related
Plossys deletes automatically requests after execution (7 days maximum), Back-up Data containing metadata (requester ID, addressee name and address) is stored 18 months.

3. Printing
3.1 Paper dashboard

Information is kept for the minimum time required to carry out the planned paper consumption analyses. In general, personal information is kept for 24 months after their emergence, to enable the individual comparability in the short- and mid-term. For the analysis of long-term developments of printing output, personal data will be aggregated and anonymised after that 24 months-period. Personal data will be deleted from the storage and only the aggregated results (e.g. total print output of a DG/PD/the Office in a month/year) will be tracked and stored for at least 10 years.

3.2 Printing - other
Requests are deleted after a maximum of 6 months.

4. Incoming Mail and parcels
Personal data are kept in Airbills 5 years and then automatically deleted (compliant with patent granting process).

5. Outgoing Mail and parcels
Personal data in Regmail are kept 5 years then automatically deleted (compliant with patent granting process).

6. Office supply
Outlook emails are kept until completion of the order for a maximum 6 months.

Data subjects and categories of personal data

Externals

Contact Information	
Phone Numbers	Working email address
Employment Information	
EPO access badge number	Office Location
Personal Identification	
Full Name	Signature
Unknown	
EPO badge validity	

Contractors

Contact Information	
Mobile Phone Number	
Personal Identification	
Full Name	

Employees

Contact Information	
Home Address	Phone Numbers
Teleworking address	Working email address
Employment Information	
Office Location	Personnel Number
Room Number	
Personal Identification	
Full Name	Signature

Recipient of the personal data

Recipients of the data 1. Logistics Centre staff working on the activities described above.
2. All contractors working on activities described above (transport companies, courier companies, drivers company's, post-offices, service contractors).

3. For the Paper dashboard, the aggregated data will be accessible to:

- Department BIT-Business Analytics CoE and staff working on the dashboard, for the administration of the Tableau tool, and managing data and follow-up
- the respective staff member, for observing and tracking their own and their team's printing behaviour.

Purpose of sharing For execution of the requested activity.

Transfer

Transfer No

Country where data might be transferred - Processor (Vendors)
Microsoft - United States

Transfer to public authority and/or International Organisation

Reasons for the transfer

Transfer mechanism(s)

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 283

Name EPO E-Learning Centre

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG0 - 02 - Communication, DG4 - 45 - CTO / BIT, DG4 - 46 - CIO / BIT

Entity Name - Controller (Entities) DG5 - 54 - Patent Intelligence

External processors

Google Ireland Limited

External processors	
Name Google Ireland Limited	

Azavista | European Patent Office | Unknown

External processors	
Name Azavista | European Patent Office | Unknown	

Description of the processing

Description The EPO E-learning Centre (also known as the Learning Management System (LMS)) is a platform that offers houses training courses to external users.

When a user registers with the e-learning centre, the user will be asked to provide certain personal data, which the EPO uses to identify the user. This includes a valid email address, which will be the user's user ID. The user will be able to modify the data (s)he enters, which will become the user's profile, at any time.

When registering for courses on the main EPO website (by using the online registration tool, which is a service provided by an external providers), the following personal data that the data subject (user) enters will be synchronised with the Learning Management System (LMS): first name, last name, city and country. The data subject's email address will be used as the user's unique identifier, i.e. will be the Data Subject's user ID.

The courses are free and no registration is required for the majority of courses. In that case, no personal data are collected.

If a user needs to register (and/or to pay) for a specific course, personal data is collected and the data subject is informed hereof, and the EPO does not proceed without the acceptance of the terms.

Data Retention Personal data is kept for as long as the user has an active account. The EPO will delete the account following a 1 year period of inactivity, or upon request of the user to cancel the account.

Purpose of Processing To create anonymised report on the platform's usage., To provide training, To collect information about the users' preferences and geographical distribution, To provide data subjects their progress

Data subjects and categories of personal data

Externals

Learning managements metrics	
Learning history	Learning plan
Contact Information	
Contact Details	Country
Personal Email	Working email address
Browsing Information	
Cookie Information	
Personal Identification	
First Name	Full Name
Surname	
Education & Skills	
Education and Training History	

Recipient of the personal data

Recipients of the data Personal data might be shared with

- EPO staff working in the EPO's Patent Intelligence Principal Directorate.

- the EPO staff and the contractors specifically selected;

- Tutors external to the EPO – hired on a contractual basis for a particular course

- the EPO's unit in charge of European and International Cooperation and with the EPO's supervisory bodies.

- In the case of training specifically for staff of national patent offices in the European Patent Organisation's member states, with those national offices' EPO co-ordination officers as part of our co-operation with those offices.

Purpose of sharing The data is shared for the purposes of administering the platform and user support. For this, it will be shared with the EPO staff and the contractors specifically selected for these purposes.

- Tutors external to the EPO – hired on a contractual basis for a particular course – receive a list of that course's participants containing their first names, last names and countries.

- For EPO-internal planning and reporting, anonymised aggregated data may be shared with the unit in charge of Academy and Patent Intelligence and with the EPO's supervisory bodies.

- In the case of training specifically for staff of national patent offices in the European Patent Organisation's member states, a list of participants in each training course is shared with those national offices' EPO co-ordination officers as part of our co-operation with those offices.

- Information on user preferences and users' geographical distribution collected to optimise technical improvements and for administering the platform and for support may be shared with EPO staff and contractors for these purposes.

Transfer

Transfer No

Country where data might be transferred - Processor (Vendors) Google Ireland Limited - Hong Kong, Google Ireland Limited - Taiwan, Google Ireland Limited - Brazil, Google Ireland Limited - Qatar, Google Ireland Limited - Indonesia, Google Ireland Limited - Singapore, Google Ireland Limited - Malaysia, Google Ireland Limited - Saudi Arabia, Google Ireland Limited - United States, Google Ireland Limited - Philippines, Google Ireland Limited - India, Google Ireland Limited - Australia, Google Ireland Limited - Chile

Transfer to public authority and/or International Organisation

Reasons for the transfer

Transfer mechanism(s)

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 286

Name Security documentation storage

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 44 - General Administration

Entity Name - Controller (Entities) DG4 - 44 - General Administration

External processors

External HSE company

External processors	
Name External HSE company	

Security Services Contractor at all EPO sites

External processors	
Name Security Services Contractor at all EPO sites	

Microsoft

External processors	
Name Microsoft	

Description of the processing

Description The Security staff of each EPO site register, archive, share and later on destroy any document required for the daily operations of the Security Services at the EPO, either manually, deleting outdated document or by automated processes programmed in the tools used for the management of documentation.
The Security Document Management System (SDMS) used for storing documents is being migrated from the current SharePoint 2019 on-premise database to OpenText, accessed using a SharePoint Online common site where links are stored and ordered using metadata fields. The expected date of completion is end of February 2025, being until then in a transitional period during which both system will work in parallel.
Additionally, the SharePoint Online site lists are connected to Tableau to display information dashboards and statistics based on the metadata stored in SharePoint Online. Access to the dashboards is restricted to the same groups that get access to the reports.
The SharePoint online site used by all EPO Security Operations staff is also the site accessed by OHS, Building Management and Maintenance for other documents related to their fields of competence (incidents related to lifts, first aid and safety incidents, fire alarms… etc.).
Each organisational unit has access to the SharePoint Online site in general but access to the linked documents in OpenText is restricted per type of document in a need-to-know basis (normally grouped per organisational unit, e.g. OHS getting access to safety and first aid or other safety related documents, Maintenance accessing lift, fire alarm or technical reports...etc.).
The types of document categories are the following (linked via SharePoint Online but stored in OpenText):
1. Security Operations Documents: This category is where the Operations Office and security staff at each EPO site archive their documents. Those include incident reports, instructions, standard operating procedures, filled forms (e.g. commission forms), etc.
2. Technical Documents: This group of documents is where all service related requests, malfunctions on safety and security systems, fire alarms, stuck in lifts reports and any other technical related reports and documents are stored. They are shared with the OHS services for safety or D Building Management/Team Building maintenance for maintenance and information.
3. Safety Documents: Any document related to health and safety issues. Those include, among others, the Office Emergency Response Plan, first aid reports, safety incident reports, emergency response team members lists, PEEP list and any other Health and Safety related documents.
The retention of each document is set in OpenText applying the retention policies per document category established by the Office.
The accuracy of the personal data in these reports and documents is checked not only by EPO permanent staff but also by an external Quality Assurance Supervisor, which ensures that only accurate data is processed and stored in this system.

Data Retention The retention applied will be 5 years in general unless the document falls under a special category that requires a longer retention period as determined by the Office (e.g. SOP's 12 years).

Purpose of Processing Personal data is processed in conformity with Circular 380, specifically Art. 2 b), whereby the President of the EPO has tasked Security Services to ensure compliance with the dispositions of the House Rules. The data registered serves to enhance the situational awareness of the security teams present in the office to provide security services and emergency assistance in an effective way. It is also used to register incidents and provide information (e.g. technical failures) that needs to be shared with other EPO departments. Additionally, the data is registered to comply with the applicable controls of the requirements established under several ISO standards on which the Office is either certified or in the process of being certified (e.g. PDCA improvement cycles of ISO 9001, 45001, 27001).

Data subjects and categories of personal data

Contractors

Health Data	
Health Data	
Contact Information	

Working email address	
Building area and site	
Building area and site	
Employment Information	
Contract Type	Department name and/or number
End Date	EPO access badge number
Grade	Language preference (of communication)
Office Location	Room Number
Start Date	
Personal Identification	
Full Name	
Unknown	
EPO badge validity	Price list for discounts

Employees

Health Data	
Health Data	
Contact Information	
Working email address	
Building area and site	
Building area and site	
Employment Information	
Contract Type	Department name and/or number
Duration of employment	End Date
Grade	Job Title Role
Office Location	Start Date
Personal Identification	
First Name	Full Name
Gender	

Unknown	
EPO badge validity	Price list for discounts
Government Identifiers	
Car registration documents	

Externals

Health Data	
Health Data	
Sensory and Electronic Information	
Time stamps from their access to the buildings	
Contact Information	
Contact Details	Mobile Phone Number
Personal Email	
Unknown	
EPO badge validity	
Personal Identification	
Date of Birth	Full Name
Government Identifiers	
National Identity Card Details	

Former Employees

Health Data	
Health Data	
Contact Information	
Mobile Phone Number	Personal Email
Personal Identification	
Gender	
Unknown	
EPO badge validity	

Recipient of the personal data

Recipients of the data 1. Security Operations documents are accessed by the D Building Management directors and Team managers and specific staff having to deal with the documents as well as the EPO internal and external security services of PD44, with the exception of a part of the library named Quality Assurance that is only accessed by EPO internal staff (Directors Building Management, Team managers and Security permanent staff).
2. Technical Documents are accessed by the group number 1 above plus the EPO technicians in charge of the service of the installations and EPO Insurance staff (D Planning), this last for analysis of risks and costs related to insurance. The Safety Expert is granted access to the documents where his expert advise is required, e.g. lift entrapments, fire alarms and similar ones.
3. Safety Documents are accessed by the same group as number 1 above plus Occupational Health staff and the Safety Expert.

For further details on how the process to access and transmit the information is established see OW-SOP-2022-004-F approved by DPO on 21.12.2022 (Link: https://teams.microsoft.com/l/message/19:meeting_ZjYyMTI1ZGUtZDcyMy00NDFmLWI2YTMtYmJhMmI3MTU3ZjM5@thread.v2/1737617833292?context=%7B%22contextType%22%3A%22chat%22%7D)

Purpose of sharing The data is only used internally by security staff and its external security contractor staff plus the organisational units mentioned above. If other recipients (e.g. Ethics and Compliance, Police, Safety Expert) request access to the personal data this will be individually asked to the Delegated Controller consulting DPL/DPO for advice.

Transfer

Transfer No

Country where data might be transferred - Processor (Vendors)
Microsoft - United States

Transfer to public authority and/or International Organisation

Reasons for the transfer

Transfer mechanism(s)

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures All personal data is processed and stored in IT applications (SharePoint) according to the security standards of EPO. These include: User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication; Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum; Logical security hardening of systems, equipment and network: 802.1x for network access, encryption of endpoint devices, AV on all devices Physical protection: EPO access controls, additional access controls to datacentre, policies to lock offices; Transmission and input controls (e.g. audit logging, systems and network monitoring): security monitoring with Splunk; Security incidence response: 24/7 monitoring for incidents, on-call security expert., For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 288

Name Job shadowing

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG0 - 02 - Communication, DG4 - 44 - General Administration, DG4 - 43 - Welfare & Remuneration

Entity Name - Controller (Entities) DG4 - 421 - Talent Acquisition and Development

External processors

Microsoft

External processors	
Name Microsoft	

Microsoft

External processors	
Name Microsoft	

Description of the processing

Description The myAbility job shadowing programme is organised by an external company and takes place once a year with approximately 3 to 5 participants.

Young professionals/graduates can express their interest for a job shadowing at the EPO and in order to assess their profiles they give their explicit agreement to share some personal data with EPO representatives through an external provider where they would have applied beforehand.

Talents are asked in advance for their consent by the external company myAbility to save their personal data (name, address, telephone number, email address, form of disability, status, field of study and companies to match with) which is a requirement for their participation.

The process comprises the following steps:
• During the application to the programme, registration at external company (myAbility): In order to participate in the programme, talents are asked in advance the consent to save their personal data in the external companyr's database (name, address, telephone number, email address, status, field of study and companies to match with) which is a requirement for their participation.
• Out of all the CVs collected, the external company shares with EPO (PD4.3 and D4.2.1) all the applications received.
• Evaluation of profiles available excluding those that are not fitting the minimum requirement (depending on the job profile) and first assessment of possible fit with the business area is carried out by D421 and PD43
• Interview with pre-selected candidates who also expressed interest in the job shadowing with the organisation is carried out by D421 and PD43
• Outcome of the "matching day". Specific number of profiles who passed the interviews and showed interest in the organisation. An Excel document with the pseudonymised profiles is created by D421 and PD43
• Recommendation of specific profile for specific area is made by D42.1 and PD43 to the EPO organisational units where the job shadowing is taking place.
• Once a candidate is nominated for a specific area, their information is shared with the line manager who is in charge /contact person for the job shadowing at the specific day.
• During the job shadowing event (information event for participants) information is shared with all participants (email address is visible in the invitation to this event), communication department, security -in case of physical event.
• After the job shadowing event (email address, first and last name, physical address) a thank you email sent by internal organisers as well as a "goodie package" to the home address.

Data Retention Personal data will be kept only for the time needed to achieve the purposes for which it is processed.
Immediately after the event, Talent Acquisition (D4211) requests the involved stakeholders to delete the personal data.
Personal data will be deleted directly after the Job shadowing takes place.

Purpose of Processing Young professionals/graduates can express their interest for a job shadowing at the EPO and in order to assess their profiles they give their explicit agreement to share some personal data with EPO representatives through an external company where they would have applied beforehand. In order to be able to decide which of the talents shall participate to the Job shadowing day at the EPO, HR representatives as well as business representatives of the EPO need some relevant information available (academy qualifications, languages, CV, etc) to enable a proper evaluation of the profiles and to allow a first assessment of the matching with the business interest.

Data subjects and categories of personal data

Externals

Health Data	
Health Data	Mobility needs
Contact Information	

Contact Details	Home Address
Personal Email	Private Phone Number
Correspondence	
Personal information provided voluntarily	
Personal Identification	
First Name	Surname
Education & Skills	
Education and Training History	

Recipient of the personal data

Recipients of the data Personal data are disclosed on a need-to-know basis to the EPO staff working in D 421 and PD 43 and the respective line manager of the organisational unit where the profile of the applicant could be considered suitable as well as to other units in order for these to carry out the necessary tasks to allow the job shadowing to take place.

Purpose of sharing Young professionals/graduates can express their interest for a job shadowing at the EPO and in order to assess their profiles they give their explicit agreement to share some personal data with EPO representatives through an external company (myAbility) where they would have applied beforehand.
In order to be able to decide which of the talents shall participate to the Job shadowing day at the EPO, HR representatives as well as business representatives of the EPO need some relevant information available (academy qualifications, languages, CV, etc) to enable a proper evaluation of the profiles and to allow a first assessment of the matching with the business interest.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors)
Microsoft - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures All personal data are stored in secure IT applications in accordance with the EPO's security standards. Appropriate levels of access are granted individually only to the above-mentioned recipients. For systems hosted on EPO premises, the following basic security measures generally apply: • User authentication and access control (e.g. role-based access control to the systems and network, principles of need-to-know and least privilege) • Logical security hardening of systems, equipment and network • Physical protection: EPO access controls, additional access controls to datacentre, policies on locking offices • Transmission and input controls (e.g. audit logging, systems and network monitoring) • Security incident response: 24/7 monitoring for incidents, on-call security expert., For personal data processed on systems not hosted on EPO premises, the providers processing the personal data have committed in a binding agreement to comply with their data protection obligations under the applicable data protection legal frameworks. The EPO has also carried out a privacy and security risk assessment. These systems are required to have implemented appropriate technical and organisational measures such as: physical security measures, access and storage control measures, securing data at rest (e.g. by encryption); user, transmission and input control measures (e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), audit logging); conveyance control measures (e.g. securing data in transit by encryption).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 291

Name Processing of personal data within the framework of the Data Protection Board tasks, duties and activities

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG0 - 07 - Data Protection Office

Entity Name - Controller (Entities) DG0 - 03 - Patent Research and Policies

External processors

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

Microsoft

External processors	
Name Microsoft	

Data Protection Board Chair and Members

External processors	
Name Data Protection Board Chair and Members	

Microsoft

External processors

Name	
Microsoft	

Description of the processing

Description The EPO's Data Protection Board (DPB) processes personal data in order to carry out the tasks and duties assigned to it by the Service Regulations for permanent and other employees of the EPO (Service Regulations), the DPR, Rules of Procedure of the Data Protection Board (RoP) and in compliance with additional operational documents governing the processing of personal data at the EPO.

The DPB fulfils a monitoring and an advisory function by providing opinions and advice on data protection related matters in response to requests for consultation from the controller, the delegated controller(s) and the EPO Data Protection Office (DPO) in the cases foreseen by the DPR. For more information on the processing of personal data by these parties, please refer to the relevant records.

Furthermore, the DPB provides an opinion where data subject files a complaint before the DPB as part of the legal redress procedure under Article 50 DPR (hereinafter "complaint proceedings"). For more information on the complaint proceedings procedure, please refer to the Rules of Procedure (RoP).

In the performance of its tasks, the DPB may process any category of personal data (including special categories of personal data) provided by EPO staff members or externals regarding themselves or third parties
in the context of the complaint proceedings. It includes information exchanged such as the description of concerns, personal case, circumstances, description of facts, evidence or arguments, opinions, assessments, etc.

Personal data are processed by the secretariat of the DPB, which is made available by the EPO (DPO), in order to assist the Chair, members and alternate members in carrying out the tasks and duties of the DPB referred to in this statement. Furthermore, the DPO might process personal data when acting upon request of the DPB in accordance with the tasks and responsibilities established under the DPR.

Personal data may be stored in one or more document management tools used by the DPB to perform its tasks, namely on the EPO's servers and/or in Microsoft Office cloud systems:

- all consultations, requests, opinions, other exchanges and related communications (together with supplementary documentation, as the case may be) received or sent by the DPB are stored in Outlook in folders separated by year and/or on SharePoint 2019 and are only accessible to authorised staff;
- opinions in the context of complaint proceedings and related documentation are additionally archived in the EPO document management tool (MatterSphere) with a specific number assigned to them;
- opinions of the DPB outside of complaint proceedings, redacted abstracts from the final decisions of the controller and the opinions of the DPB in the context of complaint proceedings may also be published on the EPO intranet and/or externally, and be made available to all staff and the general public.

For more information regarding the processing of personal data by these tools, please refer to the dedicated record(s).

The processing is not intended to be used for any automated individual decision-making.

Purpose of Processing Respond to consultations in the cases foreseen by the DPR. a. In the context of transfers of personal data to third countries and international organisations: - The DPB may provide an opinion to the President of the Office on whether the protection afforded by said third country or international organisation can be considered as adequate (Article 9(3) DPR). - In the absence of an adequate level of protection, the DPB may be consulted by the controller on the drafting of appropriate contractual clauses aiming to provide appropriate safeguards for the transfer (Article 9(5) DPR). b. In the context of Data Protection Impact Assessment (DPIA) as established by Article 38 DPR: - The DPO or the controller will consult the DPB if there is a doubt on the need to perform a DPIA (Article 43(1)(g) and 38(2) DPR). - The DPB will draw a list of the kinds of processing operations for which a DPIA is required (Article 47(2)(b) DPR). c. In the context of the removal of the Data Protection Officer from their role or termination of their appointment, the DPB provides an opinion on such removal or termination (Article 42(8) DPR). d. In the context of processing of data relating to criminal offences, criminal convictions or security measures based on Article 5(a) DPR, the DPB may need to be consulted before such processing may be carried out (Article 12(1) DPR)., Provide an opinion where data subject files a complaint before the DPB as part of the complaint proceedings. In the context of complaint proceedings personal data are processed for the following purposes: a. to register the complaint filed before the DPB using the appropriate form and to determine its receivability as foreseen by Article 5 RoP b. to forward the complaint and the attached documents (if any) to the delegated controller responsible for the processing operation which relates to the complaint, authorised parties involved in the defence of the EPO, the DPO and, where applicable, the processor in order for them to be informed of the complaint and to prepare their submissions as applicable c. if the case may be, to facilitate an amicable settlement as described in Article 8 RoP d. to provide the DPB with adequate and sufficient information to enable it to render an opinion e. if required by the circumstances of the complaint, upon the authorisation of the President of the EPO and in accordance with the Protocol on Privileges and Immunities as applicable, to co-operate with the competent national authorities, including competent national supervisory authorities or law enforcement authorities f. upon the authorisation of the President of the EPO and in accordance with the Protocol on Privileges and Immunities as applicable, to share with a court or another judicial or administrative body in the event of a suspension of complaint proceedings before the DPB pending a ruling on the same matter from the said body g. to share the reasoned opinion of the DPB with the controller and the parties involved in the procedure, including the complainant(s), legal representative(s) (if any), delegated controller(s) and authorised parties involved in the defence of the EPO and the DPO h. to archive the opinion and the final decision of the controller, rendered after reception of DPB's reasoned opinion on SharePoint 2019 and MatterSphere redacted abstracts from the final decision and from the opinion of the DPB may be published internally and/or externally by the secretariat of the DPB, Cooperate with EPO units, facilitated by the DPO, in particular with regard to organisational or other developments that are likely to have an impact on the protection of personal data within the EPO, including new administrative measures and rules.

Data Retention Personal data will be kept only for the time needed to achieve the purposes for which they are processed.

Personal data related to consultations and other exchanges will be stored in the document management tool(s) for a maximum of 5 years after the end of the consultation or end of the exchange. Opinions that are published online will be stored as long as they are operational. Upon becoming obsolete, the documents will be taken down, anonymised and archived in the document management tool(s) for an additional period of 5 years.

Personal data related to the complaint proceedings under Article 50 DPR will be stored in the document management tool(s) for a maximum of 10 years after the complaint had been withdrawn, found irreceivable or definitively resolved through a final decision taken by the controller which has not been challenged; a judgment by the Administrative Tribunal of the International Labour Organisation; a judgment issued in dispute resolution proceedings under Article 50(7) of the DPR; an arbitration award rendered in ad-hoc arbitration proceedings under Article 50(8) and 52 DPR; or an amicable settlement.

Members of the DPB shall destroy and/or erase any files or copies of files pertaining to a complaint case file within 6 months of the issue of the DPB's opinion.

In the event of a formal appeal/litigation, all data held at the time the formal appeal/litigation was initiated will be retained until the proceedings have been closed.

Data subjects and categories of personal data

Contractors

Applications' Log	
SAP Logs	
Social	
Social Media Account	Social Media Contact
Social Media History	
Sensory and Electronic Information	
Audio Information	Electronic Information
Presence Status	Thermal Information
Time stamps from their access to the buildings	Visual Information
Building area and site	
Building area and site	
Representation in EPO's Patent Granting Process	
Affiliation to Association of professional representatives	All data provided upon request for entry or change
Authorisee function	Authorisor function

EPO CDS (Client Data System) categories related to the Representation role	Representative registration number (ID)
Role in the Patent Grant Procedure	Supporting documentation
Telephony Interaction Data	
Recorded Audio File	Telephony Session Content
Telephony Session Details	Telephony Session Metadata
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name
Gender	Height
Surname	Marital Status
Nationality	Picture
Racial or Ethnic Origin	Religion/Religious Beliefs
Sexual Orientation	Signature
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
Project management experience	
Matter/Log file	
Attachments	Metadata
General	
Answers to surveys, assessments or quizzes	Any other information
Assessment and legal opinions	Input provided during the deliberation and decision-making process
Legal opinions and assessments	Nomination justificative

User association	
Workplace Welfare	
Records of Personal Properties	
Contact Information	
Contact Details	Country
Emergency Contact Details	Home Address
Mobile Phone Number	Personal Email
Phone Numbers	Previous Residence Address
Private Phone Number	Teleworking address
Working email address	
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
IDP	Instructor related data
Learning external events	Learning history
Learning plan	Social learning inputs
Device Management Data	
Account ID	AppleID for iOS/iPadOS Devices
Azure Active Directory Device ID	EAS Device ID
Encryption Keys	Intune Device ID
Intune Device Management ID	Last Logon Time
MAC Address	Managed Application Device Tag
Managed Application ID	Platform-specific IDs
Tenant ID	Windows ID for Windows Devices
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Patent Process Related Data	

Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of a patent (claims, description, drawings, abstract)
Personal data potentially included within the content of patent procedure related information and publications	
Health Insurance Information	
Insurance Policy Information	Unique Identifier for Subscriber
System Logs	
Audit Logs (a.k.a. Audit Trail)	File data (name, size and/or hash)
Firewall/Router/Switch Logs	Ports
Registry data	Running Processes
System-, Application-, Security-related Server Logs	Transaction-related Details
Web Servers Logs	
Phone Call Information	
Called Phone Number	Caller's Phone Number
Phone Call Date and/or Time	Phone Call Duration
Phone Call Interaction History	Phone Calling History
Ticketing	
Ticket related data	
Physical and/or Digital Identifiable Assets	
Digital Certificate	ICCID (Integrated Circuit Card Identification Number)
IMEI Number (International Mobile Equipment Identity)	Mobile Device Name
Mobile Device Serial Number	Mobile Device's Network Adapter MAC Adress
Operating System Version	Pod Internal Id
Smart Card Number	Videoconference Room/Equipment Identifier
Workstation Serial Number	Workstation's Hostname (Physical or Virtual)
Workstation's Network Adapter MAC address	
Biometric	
Body temperature	Facial Recognition

Fingerprint	Voice Recognition
Online invigilation data	
Audio input	Webcam captures
Background Checks	
Criminal History	Criminal Records
Drug Test Results	Reference or Background Checks
Employment Information	
Active/Inactive Indicator	Appeals Records Information
Assessment and legal opinions	Benefits and Entitlements Data
Business Unit Division	Company Entity
Contract Type	Corporate Credit or Debit Card Numbers
Department name and/or number	Disciplinary Action
Duration of employment	End Date
End Date and Reason for Termination	EPO access badge number
Exit Interview and Comments	Grade
Grievances and Complaints	Hours of Work
Job Application Details	Job Title Role
Language preference (of communication)	Line Reporting Manager
Membership in a EPO Staff Committee	Military Status
Office Location	Performance Rating
Personnel Number	Previous Work History
Record of Absence/Time Tracking/Annual Leave	Record of Maternity Leave
Room Number	Salary
Start Date	Weight
Unknown	
EPO badge validity	Identification of which membership is envisaged
Price list for discounts	

Geolocation	
Geolocation Information	
Network/application Interaction Data	
Results on phishing attempts (entered credential not processed)	Session content
Session details	Session metadata
Health Data	
Dietary requirements	Health Data
Mobility needs	
Professional Experience & Affiliations	
Affiliation	CV
Entry or deletion date as member of an association	Political Affiliation and Activities
Professional Memberships	Qualifications Certifications
Trade Union Membership	
Examination content data	
Examination marks	Examination result
Financial	
Bank Account Information	Bank Account Number
Bank details	Bank Statements
Bonus Payments	Compensation Data
Credit Card Number	Credit History
Debit Card Number	Deposit Account
Fund Reservation Requests	Information on home loans
Insurance Information	Routing Number
Browsing Information	
Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
Category	Cookie Information

IP Address	Network Interaction History
URL	Website History
User Account Information	
Account Age	Account Number
Account Password	Application Specific User Role
Membership Permissions	Ownership Permissions
Password	Password Hash
Third-party User Identifier	User ID
Government Identifiers	
Driving Licence Number	ID/Passport picture
National Identification Number	National Identity Card Details
Passport Number	Social Security Number

Employees

Applications' Log	
SAP Logs	
Social	
Social Media Account	Social Media Contact
Social Media History	
Sensory and Electronic Information	
Audio Information	Electronic Information
Presence Status	Thermal Information
Time stamps from their access to the buildings	Visual Information
Building area and site	
Building area and site	
Representation in EPO's Patent Granting Process	
Affiliation to Association of professional representatives	All data provided upon request for entry or change
Authorisee function	Authorisor function

EPO CDS (Client Data System) categories related to the Representation role	Representative registration number (ID)
Role in the Patent Grant Procedure	Supporting documentation
Telephony Interaction Data	
Recorded Audio File	Telephony Session Content
Telephony Session Details	Telephony Session Metadata
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name
Gender	Height
Surname	Marital Status
Nationality	Picture
Racial or Ethnic Origin	Religion/Religious Beliefs
Sexual Orientation	Signature
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
Project management experience	
Matter/Log file	
Attachments	Metadata
General	
Answers to surveys, assessments or quizzes	Any other information
Assessment and legal opinions	Input provided during the deliberation and decision-making process
Legal opinions and assessments	Nomination justificative

Personal data in SAP	Sensitive Personal Data in SAP
Special categories of personal data in SAP	User association
Workplace Welfare	
Records of Personal Properties	
Contact Information	
Contact Details	Country
Emergency Contact Details	Home Address
Home Leave Address	Mobile Phone Number
Personal Email	Phone Numbers
Previous Residence Address	Private Phone Number
Teleworking address	Working email address
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
Diagnostic tools' results	IDP
Instructor related data	Learning external events
Learning history	Learning plan
Ratings	Social learning inputs
Device Management Data	
Account ID	AppleID for iOS/iPadOS Devices
Azure Active Directory Device ID	EAS Device ID
Encryption Keys	Intune Device ID
Intune Device Management ID	Last Logon Time
MAC Address	Managed Application Device Tag
Managed Application ID	Platform-specific IDs
Tenant ID	Windows ID for Windows Devices
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information

Chat content	Personal information provided voluntarily
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of a patent (claims, description, drawings, abstract)
Personal data potentially included within the content of patent procedure related information and publications	
Health Insurance Information	
Insurance Policy Information	Unique Identifier for Subscriber
System Logs	
Audit Logs (a.k.a. Audit Trail)	File data (name, size and/or hash)
Firewall/Router/Switch Logs	Ports
Registry data	Running Processes
System-, Application-, Security-related Server Logs	Transaction-related Details
Web Servers Logs	
Phone Call Information	
Called Phone Number	Caller's Phone Number
Phone Call Date and/or Time	Phone Call Duration
Phone Call Interaction History	Phone Calling History
Ticketing	
Ticket related data	
Physical and/or Digital Identifiable Assets	
Digital Certificate	ICCID (Integrated Circuit Card Identification Number)
IMEI Number (International Mobile Equipment Identity)	Mobile Device Name
Mobile Device Serial Number	Mobile Device's Network Adapter MAC Adress
Operating System Version	Pod Internal Id
Smart Card Number	Videoconference Room/Equipment Identifier
Workstation Serial Number	Workstation's Hostname (Physical or Virtual)
Workstation's Network Adapter MAC address	
Biometric	

Body temperature	Facial Recognition
Fingerprint	Voice Recognition
Online invigilation data	
Audio input	Webcam captures
Background Checks	
Criminal History	Criminal Records
Drug Test Results	Reference or Background Checks
Employment Information	
Active/Inactive Indicator	Appeals Records Information
Assessment and legal opinions	Benefits and Entitlements Data
Business Unit Division	Company Entity
Contract Type	Corporate Credit or Debit Card Numbers
Department name and/or number	Disciplinary Action
Duration of employment	End Date
End Date and Reason for Termination	EPO access badge number
Exit Interview and Comments	Grade
Grievances and Complaints	Hours of Work
Job Application Details	Job Group
Job Title Role	Language preference (of communication)
Line Reporting Manager	Membership in a EPO Staff Committee
Military Status	Office Location
Performance Rating	Personnel Number
Previous Work History	Record of Absence/Time Tracking/Annual Leave
Record of Maternity Leave	Rewards history
Room Number	Salary
Start Date	Weight
Unknown	

EPO badge validity	Identification of which membership is envisaged
Price list for discounts	
Geolocation	
Geolocation Information	
Network/application Interaction Data	
Results on phishing attempts (entered credential not processed)	Session content
Session details	Session metadata
Health Data	
Dietary requirements	Health Data
Mobility needs	
Professional Experience & Affiliations	
Affiliation	CV
Entry or deletion date as member of an association	Political Affiliation and Activities
Professional Memberships	Qualifications Certifications
Trade Union Membership	
Examination content data	
Examination marks	Examination result
Family Information	
Child’s Level/Year of Studies	Child’s School Enrolment Date Start
Children's Names	Child's birthday
Composition of the family (number of dependent children/persons)	Parents' Names
Spouse's information	Spouse's name
Financial	
Bank Account Information	Bank Account Number
Bank details	Bank Statements
Bonus Payments	Compensation Data

Credit Card Number	Credit History
Debit Card Number	Deposit Account
Fund Reservation Requests	Information on home loans
Insurance Information	Routing Number
Browsing Information	
Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
Category	Cookie Information
IP Address	Network Interaction History
URL	Website History
User Account Information	
Account Age	Account Number
Account Password	Application Specific User Role
Membership Permissions	Ownership Permissions
Password	Password Hash
Third-party User Identifier	User ID
Government Identifiers	
Car registration documents	Driving Licence Number
ID/Passport picture	National Identification Number
National Identity Card Details	Passport Number
Social Security Number	

Externals

Applications' Log	
SAP Logs	
Social	
Social Media Account	Social Media Contact
Sensory and Electronic Information	

Audio Information	Electronic Information
Presence Status	Time stamps from their access to the buildings
Visual Information	
Building area and site	
Building area and site	
Representation in EPO's Patent Granting Process	
Affiliation to Association of professional representatives	All data provided upon request for entry or change
Authorisee function	Authorisor function
EPO CDS (Client Data System) categories related to the Representation role	Representative registration number (ID)
Role in the Patent Grant Procedure	Supporting documentation
Telephony Interaction Data	
Recorded Audio File	Telephony Session Content
Telephony Session Details	Telephony Session Metadata
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name
Gender	Surname
Nationality	Picture
Signature	
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
Project management experience	

Matter/Log file	
Attachments	Metadata
General	
Answers to surveys, assessments or quizzes	Any other information
Input provided during the deliberation and decision-making process	Legal opinions and assessments
Nomination justificative	User association
Contact Information	
Contact Details	Country
Emergency Contact Details	Home Address
Mobile Phone Number	Personal Email
Phone Numbers	Private Phone Number
Working email address	
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
IDP	Instructor related data
Learning external events	Learning history
Learning plan	Ratings
Social learning inputs	
European Patent Register Data	
Address	Data provided by the data subjects
Device Management Data	
Account ID	AppleID for iOS/iPadOS Devices
Azure Active Directory Device ID	EAS Device ID
Encryption Keys	Intune Device ID
Intune Device Management ID	Last Logon Time
MAC Address	Managed Application Device Tag
Managed Application ID	Platform-specific IDs

Tenant ID	Windows ID for Windows Devices
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of a patent (claims, description, drawings, abstract)
Personal data potentially included within the content of patent procedure related information and publications	
System Logs	
Audit Logs (a.k.a. Audit Trail)	File data (name, size and/or hash)
Firewall/Router/Switch Logs	Ports
Registry data	Running Processes
System-, Application-, Security-related Server Logs	Transaction-related Details
Web Servers Logs	
Phone Call Information	
Called Phone Number	Caller's Phone Number
Phone Call Date and/or Time	Phone Call Duration
Phone Call Interaction History	Phone Calling History
Ticketing	
Ticket related data	
Physical and/or Digital Identifiable Assets	
Digital Certificate	ICCID (Integrated Circuit Card Identification Number)
IMEI Number (International Mobile Equipment Identity)	Mobile Device Name
Mobile Device Serial Number	Mobile Device's Network Adapter MAC Adress
Operating System Version	Smart Card Number
Videoconference Room/Equipment Identifier	Workstation Serial Number
Workstation's Hostname (Physical or Virtual)	Workstation's Network Adapter MAC address

Biometric	
Facial Recognition	Voice Recognition
Online invigilation data	
Audio input	Webcam captures
Employment Information	
Active/Inactive Indicator	Business Unit Division
Company Entity	Contract Type
Corporate Credit or Debit Card Numbers	Department name and/or number
Duration of employment	End Date
EPO access badge number	Hours of Work
Job Title Role	Language preference (of communication)
Membership in a EPO Staff Committee	Office Location
Previous Work History	Record of Maternity Leave
Unknown	
EPO badge validity	Identification of which membership is envisaged
Price list for discounts	
Geolocation	
Geolocation	
Network/application Interaction Data	
Session content	Session details
Session metadata	
Health Data	
Dietary requirements	Health Data
Mobility needs	
Professional Experience & Affiliations	
Affiliation	CV
Entry or deletion date as member of an association	Political Affiliation and Activities

Professional Memberships	Qualifications Certifications
Examination content data	
Examination marks	Examination result
Financial	
Bank Account Information	Bank Account Number
Bank details	Credit Card Number
Debit Card Number	Deposit Account
Fund Reservation Requests	Information on home loans
Insurance Information	
Browsing Information	
Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
Category	Cookie Information
IP Address	Network Interaction History
URL	Website History
User Account Information	
Account Age	Account Number
Account Password	Application Specific User Role
Membership Permissions	Ownership Permissions
Password Hash	Third-party User Identifier
User ID	
Government Identifiers	
ID/Passport picture	National Identity Card Details
Passport Number	

Former Employees

Applications' Log	
SAP Logs	

Social	
Social Media Account	Social Media Contact
Social Media History	
Sensory and Electronic Information	
Audio Information	Electronic Information
Presence Status	Thermal Information
Time stamps from their access to the buildings	Visual Information
Building area and site	
Building area and site	
Representation in EPO's Patent Granting Process	
Affiliation to Association of professional representatives	All data provided upon request for entry or change
Authorisee function	Authorisor function
EPO CDS (Client Data System) categories related to the Representation role	Representative registration number (ID)
Role in the Patent Grant Procedure	Supporting documentation
Telephony Interaction Data	
Recorded Audio File	Telephony Session Content
Telephony Session Details	Telephony Session Metadata
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name
Gender	Height
Surname	Marital Status
Nationality	Picture

Racial or Ethnic Origin	Religion/Religious Beliefs
Sexual Orientation	Signature
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
Project management experience	
Matter/Log file	
Attachments	Metadata
General	
Answers to surveys, assessments or quizzes	Any other information
Input provided during the deliberation and decision-making process	Legal opinions and assessments
Nomination justificative	Personal Information in SAP
Sensitive Personal Data in SAP	Special Categories of Data in SAP
User association	
Workplace Welfare	
Records of Personal Properties	
Contact Information	
Contact Details	Country
Emergency Contact Details	Home Address
Home Leave Address	Mobile Phone Number
Personal Email	Phone Numbers
Previous Residence Address	Private Phone Number
Teleworking address	Working email address
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
IDP	Instructor related data
Learning external events	Learning history

Learning plan	Social learning inputs
Device Management Data	
Account ID	AppleID for iOS/iPadOS Devices
Azure Active Directory Device ID	EAS Device ID
Encryption Keys	Intune Device ID
Intune Device Management ID	Last Logon Time
MAC Address	Managed Application Device Tag
Managed Application ID	Platform-specific IDs
Tenant ID	Windows ID for Windows Devices
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of a patent (claims, description, drawings, abstract)
Personal data potentially included within the content of patent procedure related information and publications	
Health Insurance Information	
Insurance Policy Information	Unique Identifier for Subscriber
System Logs	
Audit Logs (a.k.a. Audit Trail)	File data (name, size and/or hash)
Firewall/Router/Switch Logs	Ports
Registry data	Running Processes
System-, Application-, Security-related Server Logs	Transaction-related Details
Web Servers Logs	
Phone Call Information	
Called Phone Number	Caller's Phone Number
Phone Call Date and/or Time	Phone Call Duration

Phone Call Interaction History	Phone Calling History
Ticketing	
Ticket related data	
Physical and/or Digital Identifiable Assets	
Digital Certificate	ICCID (Integrated Circuit Card Identification Number)
IMEI Number (International Mobile Equipment Identity)	Mobile Device Name
Mobile Device Serial Number	Mobile Device's Network Adapter MAC Adress
Operating System Version	Pod Internal Id
Smart Card Number	Videoconference Room/Equipment Identifier
Workstation Serial Number	Workstation's Hostname (Physical or Virtual)
Workstation's Network Adapter MAC address	
Biometric	
Body temperature	Facial Recognition
Fingerprint	Voice Recognition
Online invigilation data	
Audio input	Webcam captures
Background Checks	
Criminal History	Criminal Records
Drug Test Results	Reference or Background Checks
Employment Information	
Active/Inactive Indicator	Appeals Records Information
Benefits and Entitlements Data	Business Unit Division
Company Entity	Contract Type
Corporate Credit or Debit Card Numbers	Department name and/or number
Disciplinary Action	Duration of employment
End Date	End Date and Reason for Termination
EPO access badge number	Exit Interview and Comments

Grade	Grievances and Complaints
Hours of Work	Job Application Details
Job Group	Job Title Role
Language preference (of communication)	Line Reporting Manager
Membership in a EPO Staff Committee	Military Status
Office Location	Performance Rating
Personnel Number	Previous Work History
Record of Absence/Time Tracking/Annual Leave	Record of Maternity Leave
Rewards history	Room Number
Salary	Start Date
Weight	
Unknown	
EPO badge validity	Identification of which membership is envisaged
Price list for discounts	
Geolocation	
Geolocation Information	
Network/application Interaction Data	
Results on phishing attempts (entered credential not processed)	Session content
Session details	Session metadata
Health Data	
Dietary requirements	Health Data
Mobility needs	
Professional Experience & Affiliations	
Affiliation	CV
Entry or deletion date as member of an association	Political Affiliation and Activities
Professional Memberships	Qualifications Certifications
Trade Union Membership	

Examination content data	
Examination marks	Examination result
Family Information	
Children's Names	Parents' Names
Spouse's information	Spouse's name
Financial	
Bank Account Information	Bank Account Number
Bank details	Bank Statements
Bonus Payments	Compensation Data
Credit Card Number	Credit History
Debit Card Number	Deposit Account
Fund Reservation Requests	Information on home loans
Insurance Information	Routing Number
Browsing Information	
Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
Category	Cookie Information
IP Address	Network Interaction History
URL	Website History
User Account Information	
Account Age	Account Number
Account Password	Application Specific User Role
Membership Permissions	Ownership Permissions
Password	Password Hash
Third-party User Identifier	User ID
Government Identifiers	
Driving Licence Number	ID/Passport picture

National Identification Number	National Identity Card Details
Passport Number	Social Security Number

Prospective Employees

Applications' Log	
SAP Logs	
Social	
Social Media Account	Social Media Contact
Sensory and Electronic Information	
Audio Information	Presence Status
Time stamps from their access to the buildings	Visual Information
Building area and site	
Building area and site	
Representation in EPO's Patent Granting Process	
Affiliation to Association of professional representatives	All data provided upon request for entry or change
Authorisee function	Authorisor function
EPO CDS (Client Data System) categories related to the Representation role	Representative registration number (ID)
Role in the Patent Grant Procedure	Supporting documentation
Telephony Interaction Data	
Recorded Audio File	Telephony Session Content
Telephony Session Details	Telephony Session Metadata
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name

Gender	Height
Surname	Marital Status
Nationality	Picture
Religion/Religious Beliefs	Signature
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
Project management experience	
Matter/Log file	
Attachments	Metadata
General	
Answers to surveys, assessments or quizzes	Any other information
Input provided during the deliberation and decision-making process	Legal opinions and assessments
Nomination justificative	User association
Contact Information	
Contact Details	Country
Emergency Contact Details	Home Address
Mobile Phone Number	Personal Email
Phone Numbers	Private Phone Number
Working email address	
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
IDP	Instructor related data
Learning external events	Learning history
Learning plan	Social learning inputs
Device Management Data	
Account ID	AppleID for iOS/iPadOS Devices

Azure Active Directory Device ID	EAS Device ID
Encryption Keys	Intune Device ID
Intune Device Management ID	Last Logon Time
MAC Address	Managed Application Device Tag
Managed Application ID	Platform-specific IDs
Tenant ID	Windows ID for Windows Devices
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
System Logs	
Audit Logs (a.k.a. Audit Trail)	File data (name, size and/or hash)
Firewall/Router/Switch Logs	Ports
Registry data	Running Processes
System-, Application-, Security-related Server Logs	Transaction-related Details
Web Servers Logs	
Phone Call Information	
Called Phone Number	Caller's Phone Number
Phone Call Date and/or Time	Phone Call Duration
Phone Call Interaction History	Phone Calling History
Ticketing	
Ticket related data	
Physical and/or Digital Identifiable Assets	
ICCID (Integrated Circuit Card Identification Number)	IMEI Number (International Mobile Equipment Identity)
Mobile Device Name	Mobile Device Serial Number
Mobile Device's Network Adapter MAC Adress	Operating System Version
Videoconference Room/Equipment Identifier	Workstation Serial Number

Workstation's Hostname (Physical or Virtual)	Workstation's Network Adapter MAC address
Online invigilation data	
Audio input	Webcam captures
Background Checks	
Criminal History	Criminal Records
Drug Test Results	Reference or Background Checks
Employment Information	
Active/Inactive Indicator	Benefits and Entitlements Data
Business Unit Division	Company Entity
Contract Type	Department name and/or number
Duration of employment	End Date
End Date and Reason for Termination	EPO access badge number
Grade	Job Application Details
Job Group	Job Title Role
Language preference (of communication)	Line Reporting Manager
Membership in a EPO Staff Committee	Military Status
Office Location	Performance Rating
Previous Work History	Record of Maternity Leave
Rewards history	Salary
Start Date	Weight
Unknown	
EPO badge validity	Identification of which membership is envisaged
Price list for discounts	
Network/application Interaction Data	
Session content	Session details
Session metadata	
Health Data	

Dietary requirements	Health Data
Mobility needs	
Professional Experience & Affiliations	
Affiliation	CV
Entry or deletion date as member of an association	Political Affiliation and Activities
Professional Memberships	Qualifications Certifications
Examination content data	
Examination marks	Examination result
Financial	
Bank details	Deposit Account
Fund Reservation Requests	Information on home loans
Browsing Information	
Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
Category	Cookie Information
IP Address	Network Interaction History
URL	Website History
User Account Information	
Account Age	Account Number
Account Password	Application Specific User Role
Membership Permissions	Ownership Permissions
Password	Password Hash
Third-party User Identifier	
Government Identifiers	
ID/Passport picture	National Identity Card Details
Passport Number	

Recipient of the personal data

Recipients of the data Personal data may be disclosed to the Chair, members, alternate members and the secretariat of the DPB on a need-to-know basis and only to the extent necessary to carry out tasks and duties of the DPB. Additionally, personal data are disclosed to below mentioned recipients.

In the case of consultations, personal data may be disclosed to the controller, the delegated controller(s) responsible for the processing operation related to the consultation (including their respective Data Protection Liaisons (DPLs) if necessary), and the DPO. Strictly necessary personal data may be shared with other authorised EPO staff on a strict need-to-know basis to collect and compile information necessary for the DPB to form an opinion regarding the consultation.

In the case of exchanges with the DPO and the EPO units in particular with regard to developments likely to have impact on the processing of personal data at the EPO, personal data may be disclosed to the DPO and other authorised EPO staff involved in the exchange.

In the case of complaint proceedings personal data may be disclosed, on the need-to-know basis:
- to the parties involved in the procedure, including the complainant(s), legal representative(s) (if any), delegated controller(s), the controller, authorised parties involved in the defence of the EPO, and, where applicable, the processors, as well as to the DPO
- to the DPO and other parties that may be invited as observers during meetings of the DPB regarding the complaint
- to competent national authorities, including competent national supervisory authorities or law enforcement authorities acting within the scope of their respective competences when required by the circumstances of the complaint
- to a court or another judicial or administrative body in the event of a suspension of complaint proceedings before the DPB pending a ruling on the same matter from the said body
- to other authorised EPO staff only to the extent necessary to handle the complaint

Personal data may be stored in one or more document management tools used by the DPB to perform its tasks, notably: MatterSphere, Microsoft Outlook and SharePoint 2019. Personal data will be stored and made available in these applications strictly on a need-to-know basis and for no longer than needed to achieve the purposes for which they are processed. For more information regarding the processing of personal data by these tools, please refer to the specific data protection statements.

Personal data will only be shared with authorised persons responsible for the necessary processing operations. They will not be used for any other purposes or disclosed to any other recipients.

Purpose of sharing - To respond to consultations in the cases foreseen by the DPR
- To cooperate with EPO units, facilitated by the DPO, in particular with regard to organisational or other developments that are likely to have an impact on the protection of personal data within the EPO, including new administrative measures and rules
- To provide an opinion where data subject files a complaint as part of the legal redress procedure under Article 50 DPR

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation In the case of complaint proceedings personal data may be transferred outside the EPC contracting states:
- to competent national authorities, including competent national supervisory authorities or law enforcement authorities acting within the scope of their respective competences when required by the circumstances of the complaint
- to a court or another judicial or administrative body in the event of a suspension of complaint proceedings before the DPB pending a ruling on the same matter from the said body

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors) TRE Thomson Reuters - Luxembourg, Microsoft - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, In the context of the complaint proceedings when required by the circumstances of the complaint

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Europäisches Patentamt
European Patent Office
Office européen des brevets

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 292

Name Long-Term Care Insurance

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 431 - Compensation & Benefits, DG4 - 433 - Pension and Remuneration Services, DG4 - 422 - People Engagement and Partnership

Entity Name - Controller (Entities) DG4 - 43 - Welfare & Remuneration

External processors

SAP

External processors	
Name SAP	

Microsoft

External processors	
Name Microsoft	

Cigna

External processors	
Name Cigna	

ISRP - International Service for Remunerations and Pensions

External processors

Name
ISRP - International Service for Remunerations and Pensions

Microsoft

External processors
Name
Microsoft

ServiceNow

External processors
Name
ServiceNow

Description of the processing

Description The long-term insurance scheme is part of the social security provisions covering EPO staff and their dependants in the case they suffer from a loss of autonomy for an expected period of at least six months.

Personal data are processed when data subjects send a request (by completing an application and sending the assessment form filled out by their treating physician) for the benefits under the Long-Term Care (LTC) insurance to Cigna by e-mail or post.

Cigna is the external service provider responsible for assessing if the insured person is qualified for the LTC benefits and if so they identify the level of care and the duration of the benefits.

Cigna provides D4224 with:
- their opinion that does not contain any medical data (sent per post and per email via the HR ticketing system) and
- a sealed envelope that contains their detailed medical assessment (sent per post in a sealed envelope). This sealed envelope remains sealed i.e. it is not opened by D4224.

D4224 decide, then on behalf of the EPO President, on the base of Cigna's opinion, on the entitlement to the LTC benefits and communicate their decision to the insured person together with Cigna's sealed medical assessment.

D4224 inform HR Salary department (for active staff and their family members) and ISRP (International Service for Remunerations and Pensions) (for pensioners and their family members) about the names of the LTC beneficiaries, the level of care, the period and the amount to be paid for payment purposes.

D433 store data in OpenText: drive in an Excel file (i.e. names of the LTC beneficiaries, the level of care, the period and the amount to be paid). There are also old paper files stored in secured locked cupboard with limited access.

Cigna provides D4224 and D431 Compensation & Benefits with an annual activity report containing the names of the beneficiaries, the level of care, and the amount to be paid. The report is used for reconciliation with SAP/FIPS and billing purposes. Cigna also provides D431 with a biannual report of all beneficiaries with key dates 30 June and 31 December. This report is provided by Cigna via secured Cigna's GMS tool. It contains the names of the beneficiaries, the history of levels of care with start and end dates. The report is used for anonymised reporting purpose and to ensure consistency of the data via crosschecks against ISRP and FIPS data.

No medical data are shared between Cigna and the EPO.

Data Retention Personal data will be kept only for the time needed to achieve the purposes for which it is processed.
Data are retained for a period of maximum 13 years as of the case closure date and then are anonymized.

If the case is related to a pending litigation, data are retained until when all means of redress have been exhausted or the decision has become final. If the case is related to asbestos exposure or similar, retention has to be decided case by case.

Purpose of Processing The purpose is the administration of the the LTC insurance which is intended to provide a fixed amount of financial support to defray some of the expenses incurred if an insured person's autonomy becomes seriously impaired on a long-term basis and they therefore requires help to carry out everyday activities.

Data subjects and categories of personal data

Employees

Health Data

Health Data	
Contact Information	
Contact Details	Country
Home Address	Personal Email
Phone Numbers	
Family Information	
Children's Names	Child's birthday
Spouse's information	Spouse's name
Financial	
Bank Account Information	Bank Account Number
Bank details	
Employment Information	
Active/Inactive Indicator	Benefits and Entitlements Data
Health Insurance Information	
Insurance Policy Information	
Personal Identification	
Age	Date of Birth
Disability or Specific Condition	Full Name
Gender	Nationality
Signature	

Externals

Health Data	
Health Data	
Contact Information	
Contact Details	Country
Home Address	Personal Email
Financial	

Bank Account Information	Bank Account Number
Employment Information	
Active/Inactive Indicator	
Health Insurance Information	
Health Insurance Information	
Personal Identification	
Age	Date of Birth
Disability or Specific Condition	Full Name
Gender	Nationality
Signature	

Recipient of the personal data

Recipients of the data Personal data are disclosed on a need-to-know basis to
• D4224 to process individual LTC applications
• D431 Compensation & Benefits for reconciliation of the data with SAP/FIPS and anonymised reporting purposes
• HR Salary and SIRP for payment purposes
• D433 Pension and Remuneration Services
• HR interlocutors
• Occupational and Health Services (OHS)
• Cigna for the medical assessment and the administration of the LTC scheme.

Personal data may be disclosed to third-party service providers for maintenance and IT support purposes.

Purpose of sharing To ensure correct payment

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors) Cigna - United Kingdom, Cigna - Switzerland, ServiceNow - Netherlands, Microsoft - United States, SAP - Germany

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 293

Name IP5 Offices and Trilateral Offices websites

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 45 - CTO / BIT, DG4 - 46 - CIO / BIT

Entity Name - Controller (Entities) DG5 - 51 - European and International Affairs

Description of the processing

Description When a user visits the IP5 Offices website (EPO, USPTO, JPO, KIPO and CNIPA) and/or the Trilateral Offices website (EPO, JPO and USPTO), the EPO collects and stores the personal data assigned to that user's device in the form of data sets in order to provide them with access to the website and the requested content as well as to optimise their user experience.

The following data sets are generated on our web servers and stored in our log files:

Anonymised IP address assigned to the user's access device - date and time of the user's request for a web resource (URI)
The user's geographic location (city, district, country)

For users from the EPO's partner offices (national and international patent offices):
name and country of the partner office
Web resource (URI) requested by the user
Web resource (URI) the user previously requested (if the referrer field is available)
Browser and platform information of the user's device (if the user agent field is available)

The above data sets are stored in our database and are subject to analysis by software that helps us to better understand the usage of information provided on our websites. The purpose of such analyses is to enhance the quality of our services for the broad public. It is not done for the purpose of attributing information in the logfiles to individual users.

The storage and maintenance of data sets is a basic requirement for the provision of the website and the security of our IT systems and as such is not negotiable.

Use of cookies
Cookies are small text files sent by a website server and stored on your device (e.g. computer, tablet or phone).

When you visit the IP5 Offices website and/or the Trilateral Offices website , cookies are used for web session management, to analyse how visitors use the website and also for web browser security. They are also implemented to ensure the proper technical functioning of the website and for the purpose of tracking usage trends on an aggregated basis. For this reason, we may collect some data on your browsing experience.

This information is used to gather aggregated and anonymous statistics with a view to improving our services and your user experience. None of the cookies require your consent. The collection, aggregation and anonymisation of this data in the form of the aforementioned data sets is performed in the EPO's data centre with the necessary security measures. The analytics tool in use is Matomo. The IP5 Offices and the Trilateral Offices website also complies with the Do Not Track (DNT) option. If you enable the DNT option in your web browser, we will respect your choice, and your browsing experience on our website will not be tracked for our anonymised statistics. Instructions on how to activate this option can be found below:
Firefox
Internet Explorer
Chrome
Safari
Opera

Purpose of Processing The above data sets are stored in our database and are subject to analysis by software that helps us to better understand the usage of information provided on our websites. The purpose of such analyses is to enhance the quality of our services for the broad public. It is not done for the purpose of attributing information in the logfiles to individual users. The storage and maintenance of data sets is a basic requirement for the provision of the website and the security of our IT systems and as such is not negotiable. Use of cookies Cookies are small text files sent by a website server and stored on your device (e.g. computer, tablet or phone).

Data Retention Personal data collected via the five IP offices website will be deleted or anonymised as soon as it is no longer required for the purposes for which it has been collected, unless further processing or storage of the data is necessary in order to comply with legal obligations according to Article 5 of the EPO's DPR. It is envisaged that the Retention period will be aligned with the retention period applicable to the EPO.org website, managed by PDCOM.

Data subjects and categories of personal data

Employees

Contact Information	
Country	
Employment Information	
Company Entity	Office Location
Browsing Information	
Browser type	Browsing Time
Cookie Information	IP Address
URL	

Externals

Contact Information	
Country	
Employment Information	
Company Entity	Office Location
Browsing Information	
Browser type	Browsing Time
Cookie Information	IP Address
URL	

Recipient of the personal data

Recipients of the data The EPO does not share any information contained in cookies or data sets collected within the scope of the IP5 Offices and/or the Trilateral Offices website with any third parties.

No personal data is shared with third parties. Aggregated and anonymous information on the five IP offices website usage statistics are shared with the IP5 Offices and /or the Trilateral Offices and may be made publicly available on the IP5 Offices website and/or the Trilateral Offices website or in EPO/IP5 or EPO/Trilateralpublications.

Purpose of sharing See point 1.2 above

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 295

Name Search tool for National Patent Offices

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 46 - CIO / BIT

Entity Name - Controller (Entities) DG4 - 45 - CTO / BIT

External processors

(SDAM2) EPOSKOPIUM | DG4-45-CTO/BIT |Unknown

External processors	
Name (SDAM2) EPOSKOPIUM | DG4-45-CTO/BIT |Unknown	

IPVOLVE |DG4-45-CTO/BIT |Unknown

External processors	
Name IPVOLVE |DG4-45-CTO/BIT |Unknown	

I(P)NNOVATE | DG4-45-CTO/BIT |Unknown

External processors	
Name I(P)NNOVATE | DG4-45-CTO/BIT |Unknown	

Google Ireland Limited

External processors	
Name Google Ireland Limited	

Google Ireland Limited

External processors	
Name Google Ireland Limited	

EPOSKOPIUM |DG4-45-CTO/BIT |Unknown

External processors	
Name EPOSKOPIUM |DG4-45-CTO/BIT |Unknown	

Microsoft

External processors	
Name Microsoft	

Description of the processing

Description This record of processing activity relates to the management of the Ansera-based Search tool used for the registered users, who are patent examiners from National Patent Offices. The data in scope of the Ansera-based Search tool is limited to published patent information only. Ansera-based Search offers registered users the possibility of searching prior-art patent information data by using complex search expressions. Search-related information and annotations entered by a user are visible only to the user him/herself and are not shared to any other user, with the exception of administrator users who can access other users' annotations. NPO users enabled to use Ansera-based Search will be priorly provisioned into EPO's identity management system via the Single Access Portal. More information concerning Ansera-based Search can be found in the technical documents published on the Single Access Portal (epn.epo.org).

Purpose of Processing Personal data are processed for the following purposes: a) delivering to National Offices patent examiners a Search tool; b) operating and maintaining the Ansera-based Search tool itself; c) monitoring the Ansera-based Search tool's availability and performance; d) performing technical troubleshooting and managing security incidents; e) capacity planning and licence management purposes.

Data Retention Search Tool's user credentials are kept in Search's master system (Single Access Portal) until flagged inactive; when flagged inactive, the EPO identity management system will keep such credentials for additional 30 days and ultimately will erase them. Deletion of user credentials can be requested by emailing the National Office Support at search@epo.org.

Search data is linked to the lifecycle of the user accounts. User accounts are managed (created and deleted) by the administrator of the NPO under a user administration feature.
For the time being there are no instructions on when user accounts should be deleted; an inactive user or a user leaving does not necessarily mean deletion of data. It is currently at the discretion of the given NPO on when to ask for deleting user accounts.

Search data such as markers, bibliographic data, User Session State data, concepts, annotations, aROSS are kept under EPO EKMS encryption for an indefinite period. Annotations made by users on a dossier within the Search Tool are stored until the user deletes the dossier and can be deleted on request. The Search tool service allows users to delete application data entered by themselves, by selecting the appropriate menu option to this effect.

The IT infrastructure provides plenty of logged information related to the cloud resources located within the Ansera-based Search project. There are two default storage buckets created automatically in GCP, namely "_Default" and "_Required"; their retention periods are defined as 30 days for "_Default" and 400 days for "_Required".

The IT infrastructure has a feature to check the user's queries for eventual malicious content before such queries reach the Search application. These logs are natively available to the Search system for 30 days and forwarded to the EPO's Information Security team log repository system. A selection of GCP logs is forwarded to the EPO's Information Security team Central Log Repository; the retention period for such logs is 12 months.

Search Tool's operational application logs – including received requests – are logged for troubleshooting, performance and security monitoring purposes. Access to operational logs – within the Ansera-based Search cluster – is restricted. Such logs are not forwarded to the EPO's Information Security Central Log Repository. Search's application components which log search markers are configured to replace those entries with common placeholder text. The retention of operational application logs is 12 months.

Data subjects and categories of personal data

Externals

Network/application Interaction Data	
Session content	Session details
Session metadata	
Contact Information	
Country	Working email address
Browsing Information	
Browser type	Browser User Agent

Browsing Date and Time	Browsing Time
Cookie Information	IP Address
Search query	URL
Personal Identification	
First Name	Full Name
Surname	
User Account Information	
Application Specific User Role	Membership Permissions
User ID	
System Logs	
Audit Logs (a.k.a. Audit Trail)	File data (name, size and/or hash)
Firewall/Router/Switch Logs	Ports
Registry data	Running Processes
System-, Application-, Security-related Server Logs	Transaction-related Details
Web Servers Logs	

Recipient of the personal data

Recipients of the data Kubernetes TDA team in EPO 45326 Test & Deployment Automation;
EPO 463 IT Operations;
EPO 452 IT Cooperation project team;
EPO NOS team (National Offices Support);
EPO Ansera team and software developers;
EPO Ansera-based Search team and software developers;
Google.

Purpose of sharing 45326 Kubernetes TDA team for deployment, configuration, maintenance purposes;
463 IT Operations for deployment, configuration, maintenance purposes;
452 IT Cooperation project team for troubleshooting, dealing with support issues;
Ansera team and Ansera-based team for application support / technical troubleshooting;
Google (cloud provider) for the provision of the Google Cloud Platform infrastructure service.

Transfer

Transfer Yes

Country where data might be transferred - Processor (Vendors) Google Ireland Limited - Hong Kong, Google Ireland Limited - Taiwan, Google Ireland Limited - Brazil, Google Ireland Limited - Qatar, Google Ireland Limited - Indonesia, Google Ireland Limited - Singapore, Google Ireland Limited - Malaysia, Google Ireland Limited - Saudi Arabia, Google Ireland Limited - United States, Google Ireland Limited - Philippines, Google Ireland Limited - India, Google Ireland Limited - Australia, Google Ireland Limited - Chile, Microsoft - United States

Transfer to public authority and/or International Organisation

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Transfer mechanism(s) The recipient provided appropriate safeguards

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO takes appropriate technical and organisational measures to safeguard and protect data subjects' personal data from accidental or unlawful destruction, loss or alteration and unauthorised disclosure or access. All personal data are stored in secure IT applications in accordance with the EPO's security standards. Appropriate levels of access are granted individually only to the authorised recipients. For systems hosted on EPO premises, the following basic security measures generally apply: User authentication and access control (e.g. role-based access control to the systems and network, principles of need-to-know and least privilege); Logical security hardening of systems, equipment and network; Physical protection: EPO access controls, additional access controls to datacentre, policies on locking offices; Transmission and input controls (e.g. audit logging, systems and network monitoring); Security incident response: 24/7 monitoring for incidents, on-call security expert. For personal data processed on systems not hosted on EPO premises, the providers processing the personal data have committed in a binding agreement to comply with their data protection obligations under the applicable data protection legal frameworks. These systems are required to have implemented appropriate technical and organisational measures such as: physical security measures, access and storage control measures, securing data at rest (e.g. by encryption); user, transmission and input control measures (e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), audit logging); conveyance control measures (e.g. securing data in transit by encryption). From organisational perspective, the EPO staff and service providers dealing with personal data in the context of the Ansera-based Search tool have signed a confidentiality declaration.

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 298

Name Bot protection service (Friendly Captcha)

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG4 - 46 - CIO / BIT

External processors

Friendly Captcha GmbH

External processors	
Name Friendly Captcha GmbH	

Description of the processing

Description The EPO's bot protection service is based on the assumption that it is unprofitable for a bot operator to automatically attempt to access up websites if increased computing power is required on its systems. Friendly Captcha is a system that makes it more difficult for website visitors to use websites using automated programs and scripts (so-called "bots"). For the purpose of better protecting the EPO's publicly-facing services from bots maliciously running the account registration functionality, the EPO has integrated a Friendly Captcha program code ("widget") into the EPO websites to be protected. When a visitor attempts to enter some input text/sign in the target protected website, the widget will direct the visitor's device to the Friendly Captcha servers where the visitor's device (e.g. computer) will be asked to complete an arithmetic task ("puzzle" or "puzzle query"). The complexity of the puzzle will depend on various factors, such as whether several puzzle queries have already been placed from the IP address range of the visitor's device. The arithmetic task is solved on the visitor's device using certain system resources and sends the result to the web server of the EPO's protected site. This makes contact with Friendly Captcha's server via an interface and receives an answer as to whether the puzzle has been correctly solved on the visitor's device. Depending on the validation result, the protected website can add rules to queries from the visitor and thus continue to process or reject them.
Like other bot protection services, Friendly Captcha can make it difficult for bots to use the protected website, but it cannot prevent it.

Data Retention Personal data eventually stored in Friendly Captcha are deleted in 30 days at the latest.

Purpose of Processing EPO websites' visitors' personal data are processed to make it dynamically more difficult and discourage the usage of EPO websites by automated programs/scripts ("bots"); specifically, for protecting the account registration page against bots attempting to create accounts maliciously.

Data subjects and categories of personal data

Externals

Physical and/or Digital Identifiable Assets	
Workstation's Hostname (Physical or Virtual)	
Browsing Information	
Answer to an arithmetic problem solved on the user's device	Browser User Agent
Browsing Date and Time	IP Address
Network Interaction History	Number of requests from the (hashed) IP address per period
URL	

Recipient of the personal data

Recipients of the data Recipients of personal data are:
- Friendly Captcha (SaaS solution provider)
- Hetzner Online Gmbh (sub-contractor which does hosting and delivery of the solution)

Purpose of sharing Personal data are shared:
to Friendly Captcha for service delivery;
to Hetzner Online Gmbh for hosting and delivery;

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums)., Pseudonymisation and anonymisation: EPO users' data and Friendly Captcha's employees data are stored in the database in encrypted form. Incoming IP addresses of the client's users are only saved by Friendly Captcha in hashed form using one-way encryption.

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 300

Name Processing of International Labour Organisation Administrative Tribunal (ILOAT) complaints for external data subjects

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 47 - Procurement and Vendor Management, DG4 - 41 - Finance

Entity Name - Controller (Entities) DG0 - 08 - Employment Law and Social Dialogue Advice

External processors

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

OpenText

External processors	
Name OpenText	

Microsoft

External processors	
Name Microsoft	

OpenText

External processors

Name
OpenText

External Law Firms

External processors
Name
External Law Firms

TRE Thomson Reuters

External processors
Name
TRE Thomson Reuters

External Law Firm | European Patent Office | Consulting

External processors
Name
External Law Firm | European Patent Office | Consulting

Microsoft

External processors
Name
Microsoft

External Law Firms

External processors
Name
External Law Firms

Description of the processing

Description The delegated controller's involvement in the procedure with the Administrative Tribunal of the International Labour Organisation (herein after 'ILOAT' or 'Tribunal') and the corresponding collection (and processing) of personal data is triggered by the receipt of the notification by the Tribunal entailing the full complaint and setting the European Patent Organisation ('the Organisation') a time limit to reply. Notification is sent via email.

In order for the delegated controller to prepare the Organisation's defence, reply to the Tribunal and draft the submissions to the ILOAT, the complainant's data already collected during the previous steps of the Office's dispute settlement procedure and/or legal redress mechanism is used. Additional data is collected when it is necessary to update the complaint file. Internal fact checking is carried out by Principal Directorate Employment Law and Social Dialogue Advice (PD08) lawyers where the complainant makes a claim or brings evidence in their submission that needs to be investigated.

The elaboration of the defence of the Organisation, drafting of submissions and representation in front of the Tribunal on behalf of the Organisation might involve the transmission of relevant data electronically to external law firms.

Depending on the subject matter of the proceedings, it might require the processing of special categories of data and/or third parties' data. Such processing takes place under the condition that the processing is necessary to the adjudication of the case and proportional to the purpose (the assessment of necessity and proportionality is carried out on a case-by-case basis). Depending on the case, these data are requested in a manner that renders it anonymised or, at least, pseudonymised in a way that will not allow PD08 or delegated controller(s) further processing the data to re-identify the data subjects unless after applying these techniques, the data can no longer be meaningfully used for the performance of PD08's activities. In this case, only the minimum information strictly necessary should be processed on a case-by-case basis and in compliance with the principle of confidentiality. Techniques for anonymisation or pseudonymisation are also used when transmitting such data to the Tribunal.

Informal exchanges are conducted via email. Draft documents and other files are exchanged via email or are accessible internally through a link to the OpenText sent in the email. Data processing is done electronically as submissions are all on electronic PDF/word files, via a document management system (Mattersphere and/or OpenText). The procedural steps, including settlement initiatives, are monitored in the Tool "Caseload" (excel file).

Paper files are scanned into the system and are then stored in the physical case file.

To avoid conflict of interest, the procedure may differ for instance if a PD08 staff member initiates a complaint in front of the ILOAT.

The processing of personal data is necessary in order to address all aspects related to the consequences of the judgment, the creation of statistics, lists and legal analysis, if necessary.

Personal data concerning the complaint procedure will be stored until the last day of the 20th calendar year following the pronouncement of the Judgment.

The ILOAT publishes all decisions on the ILOAT website. These decisions are stored on the ILOAT website.

The retention time applies to both electronic and paper files.

Purpose of Processing Provide the Tribunal with adequate information to enable the judges to deliver a fair and balanced judgment, Prepare legal analysis for hierarchy (e.g., President) to identify trends and assess effectiveness of legal arguments over time, On request, the preparation of statistics and lists for the hierarchy, Identify cases that may be suitable for amicable settlement prior to the case being fixed on the Tribunal's agenda, Share necessary information with the internal business units whose involvement is necessary and required in the fulfilment of certain supplementary tasks such as execution of procurement procedures, payment of the legal fees etc., Provide the PD08 Lawyers with an understanding of the complainant's grievance and the surrounding circumstances, Provide an archive of legal reference for PD08 lawyers using MatterSphere, OpenText and the Tool (Caseload), Allow the Organisation to prepare several submissions for the ILOAT in response to the complainant's complaint, Monitor internal deadlines via 'Caseload' Tool (excel), Fulfil the final step in the EPO dispute settlement procedure and/or legal redress mechanism as foreseen by the Service Regulations (Articles 106-113 Service Regulations)

Data Retention Personal data concerning the complaint procedure will be stored until the last day of the 20th calendar year following the pronouncement of the Judgment.

The ILOAT publishes all decisions on the ILOAT website. These decisions are stored on the ILOAT website.

The retention time applies to both electronic and paper files.

Data subjects and categories of personal data

Contractors

General	
Input provided during the deliberation and decision-making process	Legal opinions and assessments
Contact Information	
Contact Details	Phone Numbers
Working email address	
Financial	
Bank Account Information	
Employment Information	
Job Title Role	
Personal Identification	
Full Name	Signature

Externals

General	
Input provided during the deliberation and decision-making process	Legal opinions and assessments
Contact Information	
Contact Details	
Employment Information	
Job Title Role	
Personal Identification	
Full Name	Signature

Recipient of the personal data

Recipients of the data - The Tribunal (ILOAT)

When applicable:

- The external data processors, e.g., external law firms representing the Office before the Tribunal.

- The complainant's legal representative / successors where they are engaged in the litigation.

- Witnesses/experts

- Internal business units on a case-by-case basis, insofar as this is compatible with the principle of confidentiality, whose involvement is necessary and required in the fulfilment of certain supplementary tasks such as execution of procurement procedures, payment of the legal fees etc.

Purpose of sharing

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation International Labour Organisation Administrative Tribunal - Switzerland

Transfer mechanism(s) The recipient provided appropriate safeguards, Data Protection EU Comm Standard Contractual Clauses

Country where data might be transferred - Processor (Vendors) TRE Thomson Reuters - Luxembourg, Microsoft - United States, External Law Firms - Switzerland, OpenText - United Kingdom

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, Provision of legal services such as drafting of submissions and for representation in front of the Tribunal on behalf of the Office

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 302

Name Internal Appeals Procedure for External Data Subjects

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 4 - Corporate Services, DG4 - 42 - People

Entity Name - Controller (Entities) DG0 - 08 - Employment Law and Social Dialogue Advice

External processors

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

OpenText

External processors	
Name OpenText	

Microsoft

External processors	
Name Microsoft	

OpenText

External processors

Name
OpenText

TRE Thomson Reuters

External processors
Name
TRE Thomson Reuters

Microsoft

External processors
Name
Microsoft

Description of the processing

Description The delegated controller's involvement in the Internal Appeals procedure and the corresponding collection (and processing) of personal data is triggered by the file of an internal appeal by (an) EPO employee(s) to the Internal Appeals Committee (ApC). The ApC notifies the delegated controller of its obligation to provide submissions necessary for the processing of the internal appeal and sets a deadline to reply.

For the Principal Directorate Employment Law and Social Dialogue Advice (PD08) Lawyers to prepare the Office's defence and draft the submissions to the ApC, personal data stored in the internal appeal file is processed. The internal appeal file mainly comprises personal data collected from the pre-litigation procedure (i.e. the management review procedure as provided for in Article 109 ServRegs). In some cases, the personal data has already been collected during previous dispute settlement procedures as envisaged under Article 106-113 ServRegs. The data is stored electronically.

Additional data is collected from the appellant's submissions and during the fact-finding exercise prior to drafting the position paper. PD08 Lawyers may contact other business units, including the line manager of the appellant where necessary for information or fact-checking purposes concerning the internal appeal. Personal data obtained through this fact- finding exercise or through Office-wide databases may be processed for the drafting of the Office's submissions.

Additional information may be processed when answering a request for information from the ApC or when carrying out a settlement initiative.

Depending on the subject matter of the proceedings, it might require the processing of special categories of data and/or third parties' data. Such processing takes place under the condition that the processing is necessary to the adjudication of the case and proportional to the purpose (the assessment of necessity and proportionality is carried out on a case-by-case basis). Depending on the case, these data are requested in a manner that renders it anonymised or, at least, pseudonymised in a way that will not allow PD08 or delegated controller(s) further processing the data to re-identify the data subjects unless after applying these techniques, the data can no longer be meaningfully used for the performance of PD08's activities. In this case, only the minimum information strictly necessary should be processed on a case-by-case basis and in compliance with the

Purpose of Processing Issuing and executing the Final Decision., Providing the hierarchy / relevant authority with adequate information on the case to enable them to make an informed, fair and balanced decision., Providing an archive of legal reference for lawyers using

principle of confidentiality. Techniques for anonymisation or pseudonymisation are also used when submitting such data to the ApC.

PD08 Lawyers draft submissions electronically. The submission is sent to the Appeals Committee Secretariat via email by the Employment Law Secretariat. This submission, having been paginated by the Appeals Committee Secretariat, becomes part of the official appeal file.

PD08 Lawyers may attend a hearing held by the ApC for the deliberation of the case. The lawyer defends the Office's position and may provide oral submissions. The employee(s), possibly represented by a lawyer, shall also be present at the hearing and defend their case before the ApC.

Depending on the case, other business units, on a case-by-case basis, insofar as this is compatible with the principle of confidentiality, may be involved in the fulfilment of certain supplementary tasks such as execution of the ApC opinion and subsequent final decision.

The delegated controller's involvement in the issuance of a Final Decision is triggered by the receipt of a reasoned opinion from the ApC pursuant to Article 110 ServRegs. PD08 is informed of the opinion of the ApC which becomes part of the appeal file stored in MatterSphere and serves as the basis for the preparation of the Final Decision pursuant to Article 110(4) ServRegs.

In order to prepare a Final Decision, the personal data included in the appeal file is processed. PD08 Lawyers process the ApC opinion and prepare a Note to the relevant authority explaining the facts of the case, the ApC opinion and the recommended Final Decision.

To avoid conflict of interest, the procedure may differ for instance if a PD08 staff member initiates an appeal in front of the ApC.

Informal exchanges are conducted via email. Draft documents and other files are exchanged via email or are accessible internally through a link to the shared drive / OpenText sent in the email.

Data processing is done electronically as submissions, requests for information, statistics and legal analysis are all stored on electronic PDF, word or excel files and stored on MatterSphere or on the OpenText.

The procedural steps, including settlement initiatives, are monitored in the Tool "Caseload" (excel).

Prior to mid-2018 Paper files were scanned into the system and then stored in the physical case file. The creation of physical files has ceased since mid-2018.

The processing of personal data is necessary in order to address all aspects related to the internal case file (fact-finding), the consequences of the Final Decision, the creation of statistics, lists and the legal analysis, if necessary.

Data Retention Personal data will be kept only for the time needed to achieve the purposes for which it is processed. Personal data concerning the appeals procedure will be stored until the last day of the 20th calendar year following the issuance of the final decision.

The retention time applies to both electronic and paper files.

MatterSphere, OpenText and the tool 'Caseload' tool (Excel)., The monitoring of deadlines via 'Caseload' tool (excel)., On request, the preparation of statistics and lists for the hierarchy., The fulfilment of the internal appeals procedure under Article 110 Service Regulations., Establishing all of the facts to provide comprehensive submissions to the ApC on the Office's behalf., Identifying recurring and systemic legal issues., Contacting the appellant(s) and notifying them of the Final Decision., Providing PD08 Lawyers with an understanding of the appellant's grievance and the surrounding circumstances., Identifying cases that may be suitable for amicable settlement., The preparation of legal analysis for hierarchy and other business units to identify trends and assess the effectiveness of legal arguments over time., Providing the ApC with adequate information to enable the presiding Committee members to deliver a reasoned opinion., The reassessment of a case depending on the ApC opinion.

Data subjects and categories of personal data

Externals

General	
Input provided during the deliberation and decision-making process	Legal opinions and assessments
Contact Information	
Contact Details	
Employment Information	
Job Title Role	
Personal Identification	
Full Name	Signature

Recipient of the personal data

Recipients of the data Members of the Internal Appeals Committee and the Appeals Committee Secretariat.

The appellant's legal representative / successors where they are engaged in the litigation.

Witnesses/experts.

Internal business units whose involvement is necessary and required by PD08, on a case-by-case basis, insofar as this is compatible with the principle of confidentiality, in the fulfilment of certain supplementary tasks such as execution of the ApC opinion and subsequent final decision.

Purpose of sharing

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards, Data Protection EU Comm Standard Contractual Clauses

Country where data might be transferred - Processor (Vendors) Microsoft - United States, TRE Thomson Reuters - Luxembourg, OpenText - United Kingdom

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 304

Name Data Protection Board Complaints Procedure for External Data Subjects

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG0 - 07 - Data Protection Office, DG4 - 47 - Procurement and Vendor Management, DG0 - 01 - President`s Office - Vice-President, DG4 - 41 - Finance

Entity Name - Controller (Entities) DG0 - 08 - Employment Law and Social Dialogue Advice

External processors

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

OpenText

External processors	
Name OpenText	

Microsoft

External processors	
Name Microsoft	

OpenText

External processors

Name
OpenText

External Law Firms

External processors
Name
External Law Firms

TRE Thomson Reuters

External processors
Name
TRE Thomson Reuters

Microsoft

External processors
Name
Microsoft

Description of the processing

Description The involvement of the Principal Directorate Employment Law and Social Dialogue Advice (PD 08) in the complaint procedure before the Data Protection Board ('DPB') and the corresponding collection (and processing) of personal data is triggered by the filing of a complaint by (an) data subject(s) covered by Article 1 Service Regulations to the DPB in accordance with the Implementing Rules for Articles 1b and 32a of the Service Regulations ('Data Protection Rules' or 'DPR').

The Secretariat of the DPB registers the complaint and notifies the controller and the Chair of the DPB of the complaint. The Secretariat of the DPB informs PD08 and communicates the deadline for submission on considerations regarding the complaint.

For the PD08 Lawyers to prepare the controller's defence and prepare the submissions to the DPB, personal data stored on the complaint file is processed. The data is stored electronically.

Additional information may be processed when answering a request for information from the DPB or when carrying out a settlement initiative.

Depending on the case, other business units, on a case-by-case basis, insofar as this is compatible with the principle of confidentiality, may be involved in the fulfilment of certain supplementary tasks, such as execution of the DPB opinion and subsequent final decision.

The elaboration of the defence of the controller, drafting of submissions and representation in front of the DPB on behalf of the controller might involve the transmission of relevant data electronically to external law firms.

Depending on the subject matter of the proceedings, it might require the processing of special categories of data and/or third parties' data.

Purpose of Processing Providing an archive of legal reference for lawyers., Providing the DPB with adequate information to enable the

Such processing takes place under the condition that the processing is necessary to the adjudication of the case and proportional to the purpose (the assessment of necessity and proportionality is carried out on a case-by-case basis). Depending on the case, these data are requested in a manner that renders it anonymised or, at least, pseudonymised in a way that will not allow PD08 or delegated controller(s) further processing the data to re-identify the data subjects unless after applying these techniques, the data can no longer be meaningfully used for the performance of PD08's activities. In this case, only the minimum information strictly necessary should be processed on a case-by-case basis and in compliance with the principle of confidentiality. Techniques for anonymisation or pseudonymisation are also used when submitting such data to the DPB.

Upon receipt of a reasoned opinion from the DPB, PD 08 Lawyers process the DPB opinion and prepare a Note to the competent authority explaining the facts of the case, the DPB opinion and the recommended Final Decision. Such Note is shared with the competent authority together with the DPB opinion and the recommended Final Decision to enable them to make an informed, fair and balanced decision. Once the Final Decision is issued, the Secretariat of the DPB receives a copy of the Final Decision via email.

A copy of the Final Decision is also stored in MatterSphere and the OpenText. In the event a Note to the President is required, it is communicated to the Appointing Authority via the CommonLog. Informal communication together with draft documents and other files are exchanged via email.

To avoid conflict of interest, the procedure may differ for instance if a PD08 staff member initiates a complaint before the DPB.

The data collected may also be used for other purposes by the PD08 as e.g. to compile statistics and/or lists and carry out legal analysis for the hierarchy or other business units.

Data processing is done electronically as submissions, requests for information and (legal) analyses are all stored on electronic pdf, word or excel files and stored on MatterSphere, or OpenText.

Please note that, to avoid conflict of interest, the procedure may differ for instance if the decision challenged before the DPB is taken by the delegated controller of the PD08 or if a PD08 staff member initiates a complaint in front of the DPB.

The processing of personal data is necessary in order to address all aspects related to the complaint file, the consequences of the Final Decision, the creation of statistics, lists and the legal analysis, if necessary.

Data Retention Personal data concerning the complaint procedure will be stored until the last day of the 10th calendar year after closure of the case.

The retention time applies to both electronic and paper files.

DPB members to deliver a reasoned opinion., Providing the hierarchy / competent authority with adequate information on the case to enable them to make an informed, fair and balanced decision., Share necessary information with the internal business units whose involvement is necessary and required in the fulfilment of certain supplementary tasks such as execution of procurement procedures, payment of the legal fees etc., Issuing and where required, executing the Final Decision., Identifying recurring and systemic legal issues., The fulfilment of the complaint procedure before the DPB under Article 50 of the Data Protection Rules., Contacting the complainant(s) and notifying them of the Final Decision., Providing PD08 with an understanding of the complainant's grievance and the surrounding circumstances., Identifying cases that may be suitable for amicable settlement., On request, the preparation of statistics for the hierarchy., The preparation of legal analysis for hierarchy and other business units to identify trends and assess the effectiveness of legal arguments over time., Establishing all of the facts to provide comprehensive submissions to the DPB on the controller's behalf.

Data subjects and categories of personal data

Contractors

General	
Input provided during the deliberation and decision-making process	Legal opinions and assessments
Contact Information	

Contact Details	Phone Numbers
Working email address	
Financial	
Bank Account Information	
Employment Information	
Job Title Role	
Personal Identification	
Full Name	Signature

Externals

General	
Input provided during the deliberation and decision-making process	Legal opinions and assessments
Contact Information	
Contact Details	
Employment Information	
Job Title Role	
Personal Identification	
Full Name	Signature

Recipient of the personal data

Recipients of the data - Members of the Data Protection Board
- Secretariat of the Data Protection Board
- Delegated controller concerned

When applicable:
- External law firm representing the delegated controller
- Complainant's legal representative where they are engaged in the procedure
- Witnesses / experts
- Internal business units involved in the case or business units whose involvement is necessary and required by PD08 on a case-by-case basis, insofar as this is compatible with the principle of confidentiality, in the fulfilment of certain supplementary tasks such as execution of the DPB opinion and subsequent final decision.

Purpose of sharing The personal data of data subjects are shared with the above mentioned recipients for the following purposes:

- The fulfilment of the complaint procedure before the DPB under Article 50 of the Data Protection Rules.
- Establishing all of the facts to provide comprehensive submissions to the DPB on the controller's behalf.
- Providing the DPB with adequate information to enable the DPB members to deliver a reasoned opinion.
- Representing the controller's position for assessment by the DPB.
- Identifying cases that may be suitable for amicable settlement.
- Issuing and where required, executing the Final Decision.
- Concluding the DPB complaint procedure.
- Share necessary information with the internal business units whose involvement is necessary and required in the fulfilment of certain supplementary tasks such as execution of procurement procedures, payment of the legal fees etc.

Transfer

Transfer Yes

Country where data might be transferred - Processor (Vendors) TRE Thomson Reuters - Luxembourg, External Law Firms - Switzerland, Microsoft - United States, OpenText - United Kingdom

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards, Data Protection EU Comm Standard Contractual Clauses

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 305

Name Amicable Settlement Attempt for External Data Subjects

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 41 - Finance, DG0 - 06 - Appeal Committee Secretariat, DG4 - 42 - People

Entity Name - Controller (Entities) DG0 - 08 - Employment Law and Social Dialogue Advice

External processors

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

OpenText

External processors	
Name OpenText	

Microsoft

External processors	
Name Microsoft	

OpenText

External processors

Name
OpenText

TRE Thomson Reuters

External processors
Name
TRE Thomson Reuters

Microsoft

External processors
Name
Microsoft

Description of the processing

Description The data controller's involvement in the amicable settlement procedure and the corresponding collection and processing of personal data is triggered at the pre-litigation and/or litigation stages as defined in Article 106-113 Service Regulations for permanent and other employees.

Principal Directorate Employment Law and Social Dialogue Advice (PD08) Lawyers identify cases that may be appropriate for settlement. Efforts to reach an amicable settlement focus mainly on cases before they are placed on the agenda of the Internal Appeals Committee ('ApC') or the Administrative Tribunal of the International Labour Organization ('ILOAT'). The ApC can also enquire about the possibility of an amicable settlement in the cases placed on their agenda. Prior to the commencement of an ILOAT session, a similar procedure conducted by the ILOAT Registrar applies.

PD08 Lawyers process the personal data contained in the communications and submissions put forward during pre-litigation or litigation to determine whether the case is appropriate for settlement and if so, on what basis/terms.

The data processed for the amicable settlement is taken from the case file stored on the document management systems. PD08 lawyers check the facts of the case for accuracy. Additional data is collected when it is necessary to update the file.

Depending on the subject matter of the proceedings, it might require the processing of special categories of data and/or third parties' data. Such processing takes place under the condition that the processing is necessary to the adjudication of the case and proportional to the purpose (the assessment of necessity and proportionality is carried out on a case-by-case basis). Depending on the case, these data are requested in a manner that renders it anonymised or, at least, pseudonymised in a way that will not allow PD08 or delegated controller(s) further processing the data to re-identify the data subjects unless after applying these techniques, the data can no longer be meaningfully used for the performance of PD08's activities. In this case, only the minimum information strictly necessary should be processed on a case-by-case basis and in compliance with the principle of confidentiality. Techniques for anonymisation or pseudonymisation are also used when submitting such data to another delegated controller(s), if required.

A proposal for a settlement attempt including a statement of reasons is

prepared by the PD08 Lawyers and sent to the hierarchy for approval by e-mail, or in a Note to the hierarchy.

In the event a settlement proposal is approved by hierarchy, the settlement proposal is prepared by PD08 Lawyers and sent to the employee concerned involved by the Employment Law Secretariat via email including an invitation to the employee concerned, or their (legal) representative / successor, if applicable to enter settlement negotiations. The Employment Law Secretariat may send and receive further email correspondences to/from the employee concerned or their (legal) representative / successor.

Settlement negotiations may take place between the PD08 staff, the operational unit involved, the Human Resources Business Partner ('HRBP') and the employee concerned and their (legal) representative / successor in writing, in person or via (video) call (Microsoft Teams, Zoom).

Depending on the case, other business units may be involved in the fulfilment of certain supplementary tasks, such as facilitation of settlement negotiations and execution of the settlement.

The entire settlement procedure is strictly confidential.

If the person concerned accepts or rejects a settlement attempt, the settlement procedure ends.

Depending on the case, the ApC Secretariat or the ILOAT Registrar will be informed about the outcome of the settlement procedure.

Informal exchanges are conducted via email. Draft documents and other files are exchanged via email or are accessible internally through a link to the shared drive / OpenText sent in an email.

Data processing is done electronically as the data including the case file with all correspondence between the data subject and the Office inviting them to settlement negotiations are all stored on electronic PDF, word or excel files and stored on MatterSphere or on the OpenText. In the event a settlement attempt must be approved by the President, the NttPs are stored also on the CommonLog.
The procedural steps, including settlement initiatives and the outcome of amicable settlement attempts is recorded on the tool 'Caseload' (excel) by the Employment Law Secretariat.
Employment Law Secretariat maintains a database of cases (Excel) appropriate for settlement and the status / success of amicable settlement negotiations.
Paper files are scanned into the system and are then stored in the physical case file. The creation of physical files has ceased since mid-2018.

To avoid conflict of interest, the procedure may differ for instance if a PD08 staff member is a party of the settlement procedure.

The processing of personal data is necessary in order to address all aspects related to the consequences of the settlement, the creation of statistics and lists and the legal analysis, if necessary.

Data Retention Personal data concerning the settlement procedure will be stored until the last day of the 10th calendar year after closure of the settlement procedure.

The retention time applies to both, electronic and paper files.

Purpose of Processing Providing the employee concerned with sufficient and coherent reasoning in the conclusion of the settlement procedure., Prepare legal analysis for hierarchy to identify trends and assess effectiveness of legal arguments over time., Providing PD08 Lawyers with an understanding of the legal issue and the surrounding circumstances., The monitoring of deadlines., Providing an archive of legal reference for PD08 Lawyers., The amicable settlement of disputes as provided for in Article 6 of the Impl. Rules to Article 106-113 ServRegs., Preparing statistics, lists and analysis for the hierarchy, if requested., The promotion of social dialogue., Establishing all of the facts and providing comprehensive legal input to the competent authority taking the decision on the settlement proposal.

Data subjects and categories of personal data

Externals

General	
Input provided during the deliberation and decision-making process	Legal opinions and assessments
Contact Information	
Contact Details	
Employment Information	
Job Title Role	
Personal Identification	
Full Name	Signature

Recipient of the personal data

Recipients of the data Recipients within the EPO:
• Members of the Internal Appeals Committee
• Appeals Committee Secretariat
• Internal business units (e.g., HRBPs, Finance) whose involvement is necessary and required in the fulfilment of certain supplementary tasks such as the facilitation of settlement negotiations, the execution of the settlement and the preparation of statistics, lists and analysis, on a case-by-case basis, insofar as this is compatible with the principle of confidentiality.

Recipients outside the EPO:
• The Tribunal (ILOAT)
• The external law firms representing the EPO before the ILOAT, when applicable
• The (legal) representative / successors where they are engaged in settlement negotiations.

Purpose of sharing

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation International Labour Organisation Administrative Tribunal - Switzerland

Transfer mechanism(s) The recipient provided appropriate safeguards, Data Protection EU Comm Standard Contractual Clauses

Country where data might be transferred - Processor (Vendors) TRE Thomson Reuters - Luxembourg, Microsoft - United States, OpenText - United Kingdom

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, If the data controller's involvement in the amicable settlement procedure and the corresponding collection and processing of personal data is triggered at the litigation stages before ILOAT (e.g., upon the request of ILOAT), specific categories of personal data is provided to the ILOAT.

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Europäisches Patentamt
European Patent Office
Office européen des brevets

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 309

Name Disciplinary Procedure for External Data Subjects

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG0 - 01 - President`s Office - Vice-President

Entity Name - Controller (Entities) DG0 - 08 - Employment Law and Social Dialogue Advice

External processors

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

OpenText

External processors	
Name OpenText	

OpenText

External processors	
Name OpenText	

Microsoft

External processors

Name
Microsoft

TRE Thomson Reuters

External processors
Name
TRE Thomson Reuters

Microsoft

External processors
Name
Microsoft

Description of the processing

Description Initiation of proceedings before the Disciplinary Committee:

The appointing authority's involvement in the disciplinary procedure and the corresponding collection (and processing) of personal data is triggered when the appointing authority becomes aware of evidence or indications of misconduct. The appointing authority will determine whether the Disciplinary Committee must be convened.

Principal Directorate Employment Law and Social Dialogue Advice (PD08) Lawyers prepare a report which is then given on behalf of the appointing authority to the Disciplinary Committee. This report is also shared with the person concerned and their (legal) representative, if any.

The person concerned may also prepare submissions for the Disciplinary Committee. Submissions are made available to the concerned parties, the Disciplinary Committee and the PD08 Lawyer involved. The submissions are sent via email and stored electronically (subject to restricted access). All submissions are provided before a confidential hearing takes place. The hearing is attended by the person concerned, their (legal) representative, the Disciplinary Committee, witnesses and a PD08 Lawyer.

The Disciplinary Committee processes the submissions to prepare a reasoned opinion.

The Disciplinary Committee issues a reasoned opinion which is then shared with the person concerned and their (legal) representative, the appointing authority and PD08 Lawyers. PD08 Lawyers process the opinion and draft a note to the appointing authority containing legal advice on the Decision. The appointing authority processes the legal input and the Disciplinary Committee opinion when making an informed decision. The person concerned is heard by the appointing authority before the issuance of an informed decision. A Decision is signed by the appointing authority and sent by the secretariat in charge to the person concerned and their (legal) representative via email.

Disciplinary Proceedings before the competent authority:

The competent authority's involvement in the disciplinary procedure and the corresponding collection (and processing) of personal data is

triggered when the appointing authority becomes aware of evidence or indications of misconduct. The appointing authority may decide to conduct disciplinary proceedings but not to convene the Disciplinary Committee depending on the seriousness of the allegations.

PD08 Lawyers process the DEC report to create a letter on behalf of the competent authority. This letter is shared with the appointing authority, the person concerned and their (legal) representative, if any. Electronic submissions are exchanged and sent via email. The correspondences are sent to the person concerned and their (legal) representative, and received by the competent authority then shared with PD08. Files are stored electronically and are subject to restricted access.

Before the decision is taken, the person concerned is given the opportunity to state their case, orally or in writing. The competent authority may hold a confidential meeting attended by the person concerned, their (legal) representative, witnesses, if any and a PD08 Lawyer, depending on the case. Witness statements are also processed and stored electronically, subject to restricted access.

PD08 Lawyers process all submissions to provide legal advice to the competent authority on the Decision by means of a note to the hierarchy. The signed decision of the competent authority is sent by e-mail to the person concerned and their (legal) representative, if any, by the secretariat in charge.

General remarks applicable to both procedures

The processing of personal data is necessary in order to deal with all aspects related to the case and take a reasoned Decision on the case, the creation of lists and legal analysis, if necessary.

Correspondences are conducted on Outlook (email). Documents are sent via email or accessible using a link to the shared drive / OpenTextwhich is accessible to authorised persons.

Depending on the subject matter of the proceedings, it might require the processing of special categories of data and/or third parties' data. Such processing takes place under the condition that the processing is necessary to the adjudication of the case and proportional to the purpose (the assessment of necessity and proportionality is carried out on a case-by-case basis). Depending on the case, these data are requested in a manner that renders it anonymised or, at least, pseudonymised in a way that will not allow PD08 or delegated controller(s) further processing the data to re-identify the data subjects unless after applying these techniques, the data can no longer be meaningfully used for the performance of PD08's activities. In this case, only the minimum information strictly necessary should be processed on a case-by-case basis and in compliance with the principle of confidentiality. Techniques for anonymisation or pseudonymisation are also used when submitting such data to the Disciplinary Committee.

The procedure may differ if a staff member involved in the decision making procedure concerning disciplinary procedure has a conflict of interest.

The entire disciplinary procedure is strictly confidential.

The data collected may also be used for other purposes by the delegated controller as e.g. to compile statistics, lists and carry out legal analysis for the hierarchy or other business units.

Purpose of Processing Prepare statistics and legal analysis for hierarchy to identify trends and assess effectiveness of legal arguments over time., Identify cases that may be suitable for amicable settlement prior to the case being fixed on the Disciplinary Committee's agenda., Prepare a Note to the appointing authority containing legal advice to make a reasoned Decision., Provide the Disciplinary Committee with adequate information to enable them to deliver a fair and balanced opinion., Provide the PD08 Lawyers with an understanding of the alleged misconduct of a person concerned and the surrounding circumstances, and to determine the possible sanction to be imposed., Allow PD08 Lawyers to prepare reports/submissions on behalf of the Office for the consideration of the Disciplinary Committee., Allow the person concerned a fair opportunity to defend themselves against sanctioning., Provide an archive of legal reference for PD08 lawyers.

Data Retention Personal data concerning the disciplinary proceedings will be stored until the last day of the 10th calendar year after closure of the case.

The retention time applies to both electronic and paper files.

Data subjects and categories of personal data

Externals

General	
Input provided during the deliberation and decision-making process	Legal opinions and assessments
Contact Information	
Contact Details	
Employment Information	
Job Title Role	
Personal Identification	
Full Name	Signature

Recipient of the personal data

Recipients of the data Secretariat and Members of the Disciplinary Committee.

Witnesses/experts

Internal business units whose involvement is necessary and required, on a case-by-case basis, insofar as this is compatible with the principle of confidentiality, in the fulfilment of certain supplementary tasks such as:

(i) the provision of information assisting in the investigation into the misconduct,
(ii) the preparation of the decision on the proceedings and
(iii) the execution of the sanction imposed.

Purpose of sharing

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards, Data Protection EU Comm Standard Contractual Clauses

Country where data might be transferred - Processor (Vendors) Microsoft - United States, TRE Thomson Reuters - Luxembourg, OpenText - United Kingdom

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 310

Name Professional Incompetence Procedure for External Data Subjects

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) Chairperson of the Joint Committee on Articles 52 and 53

Entity Name - Controller (Entities) DG0 - 08 - Employment Law and Social Dialogue Advice

External processors

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

OpenText

External processors	
Name OpenText	

Microsoft

External processors	
Name Microsoft	

OpenText

External processors

Name
OpenText

TRE Thomson Reuters

External processors
Name
TRE Thomson Reuters

Microsoft

External processors
Name
Microsoft

Description of the processing

Description Referral of the case to the Joint Committee

The competent authority's involvement in the professional incompetence procedure and the corresponding collection (and processing) of personal data is triggered by the President's decision to refer the case to the Joint Committee.

After three consecutive annual appraisals indicating unacceptable performance, the employee is offered the opportunity to remedy their lack of ability and efficiency. If the employee's performance does not improve, the Reporting Officer and the Counter-Signing Officer may escalate the case to the President. The case is processed by Principal Directorate Employment Law and Social Dialogue Advice (PD 08) Lawyers in order to advise the President on the seriousness of the case and whether to refer the case to the Joint Committee.

PD08 Lawyers process the evidence put forward by the Reporting Officer and Counter-signing Officer and prepare a reasoned proposal for appropriate measures on behalf of the President to the Joint Committee. The report from the appointing authority is also provided to the employee to which they are entitled to respond and request a complete copy of their personal file and all other documentation relevant to the proceedings. All files are prepared electronically.

The Joint Committee may order an inquiry in which they seek additional information. Both sides can make submissions and can respond to the submission of the other side. Witnesses may provide evidence during the proceedings.

The Joint Committee issues a signed reasoned opinion and transmits its reasoned opinion to the President and to the employee concerned.

PD08 Lawyers process the reasoned opinion and prepare a Note to the hierarchy outlining the appropriate sanction together with a recommended final decision. The final decision signed by the President is communicated to the employee concerned via email sent by the Employment Law Secretariat or the President's Office.

Professional Incompetence Proceedings before the relevant authority

The relevant authority's involvement in the incompetence procedure and the corresponding collection (and processing) of personal data is triggered by the President's decision not to refer the case to the Joint Committee. The relevant authority is entrusted to consider the case

and to make a reasoned decision.

Following the employee's failure to remedy their lack of ability and efficiency, the Reporting Officer and Counter-Signing Officer may escalate the case to the President after three consecutive annual appraisal reports indicating unacceptable performance. This communication is done electronically. PD08 Lawyers process the evidence put forward by the Reporting Officer and Counter-signing Officer and prepare a reasoned proposal for appropriate measures for the relevant authority. The report from the appointing authority is also provided to the employee to which they are entitled to respond and request a complete copy of their personal file and all other documentation relevant to the proceedings. All files are prepared electronically.

PD08 Lawyers draft submissions on behalf of the Office. Any email correspondences are secured and sent and received by the Employment Law Secretariat. The relevant authority presides over an internal hearing attended by the employee. Witnesses may be heard, and witness statements processed and stored electronically on MatterSphere. The hearing is confidential.

PD08 Lawyers may provide the relevant authority with legal advice which is communicated in a Note together with a recommended final decision and sent by the Employment Law Secretariat via email. The final decision issued by the relevant authority is communicated to the employee concerned via email by the Employment Law Secretariat.

Depending on the case, other business units may be involved in the fulfilment of certain supplementary tasks, such as provision of information assisting in the examination into the unacceptable overall performance.

Depending on the subject matter of the proceedings, it might require the processing of special categories of data and/or third parties' data. Such processing takes place under the condition that the processing is necessary to the adjudication of the case and proportional to the purpose (the assessment of necessity and proportionality is carried out on a case-by-case basis). Depending on the case, these data are requested in a manner that renders it anonymised or, at least, pseudonymised in a way that will not allow PD08 or delegated controller(s) further processing the data to re-identify the data subjects unless after applying these techniques, the data can no longer be meaningfully used for the performance of PD08's activities. In this case, only the minimum information strictly necessary should be processed on a case-by-case basis and in compliance with the principle of confidentiality. Techniques for anonymisation or pseudonymisation are also used when submitting such data to the Joint Committee.

To avoid conflict of interest, the procedure may differ for instance if a PD08 staff is the employee concerned in the professional incompetence procedure.

The processing of personal data is necessary in order to address all aspects related to the consequences of the procedure, the creation of lists for archiving and monitoring of internal deadlines and legal analysis, if necessary.

Data Retention Personal data concerning the professional incompetence proceedings will be stored until the last day of the 10th calendar year after closure of the case.

Purpose of Processing Identify cases that may be suitable for amicable settlement prior to the case being fixed on the Joint Committee's agenda., Provide PD08 Lawyers with an understanding of the alleged professional incompetence and the surrounding circumstances, and to determine the possible sanction to be imposed., Prepare legal analysis for hierarchy to identify trends and assess effectiveness of legal arguments over time., Allow PD08 lawyers to prepare submissions on behalf of the Office for the consideration of the Joint Committee and the competent authority., Prepare statistics and lists for the hierarchy on request., Prepare a Note to the President containing legal advice to make a reasoned Decision., Provide an archive of legal reference for PD08 lawyers., Provide the Joint Committee with adequate information to enable them to deliver a fair and balanced opinion.

Data subjects and categories of personal data

Externals

General	
Input provided during the deliberation and decision-making process	Legal opinions and assessments
Contact Information	
Contact Details	
Employment Information	
Job Title Role	
Personal Identification	
Full Name	Signature

Recipient of the personal data

Recipients of the data a. Members of the Joint Committee
b. The person assisting the employee concerned where they are engaged in the proceedings
c. Witnesses/experts

Internal business units (inter alia HRBP, HR services, Finance, Line Managers) involved in the case or business units whose involvement is necessary and required in the fulfilment of certain supplementary tasks such as the provision of information or a witness statement and assisting in the examination into the unacceptable overall performance, on a case-by-case basis, insofar as this is compatible with the principle of confidentiality.

Purpose of sharing

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards, Data Protection EU Comm Standard Contractual Clauses

Country where data might be transferred - Processor (Vendors) OpenText - United Kingdom, Microsoft - United States, TRE Thomson Reuters - Luxembourg

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 318

Name User satisfaction surveys on search services, on examination services, final actions and publication as well as on opposition services

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG5 - 53 - Patent Law and Procedures

Entity Name - Controller (Entities) DG1 - 15 - Customer Journey and KAM, DG1 - 1 - Patent Granting Process

External processors

BERENT Deutschland GmbH

External processors	
Name BERENT Deutschland GmbH	

WeTransfer

External processors	
Name WeTransfer	

WeTransfer

External processors	
Name WeTransfer	

BERENT Deutschland GmbH

External processors

Name
BERENT Deutschland GmbH

Description of the processing

Description The user satisfaction surveys are targeted at applicants and external representatives who have had dealings with the EPO, and they are carried out by external processors. The sample of potential respondents prepared by the EPO normally includes data only from publicly available sources. Should this data not be sufficient for the external processor to contact the potential respondent, the external processor looks for further contact details in other publicly available sources.

Statistically solid and representative figures about user satisfaction with core services of the EPO is an ISO 9001 requirement of EPO's certified Quality Management System and can only be achieved through quantitative surveys with a large number of interviews among both applicants and external representatives.

The objective of this processing activity is to measure the level of users' satisfaction e.g. by type of user in order to identify the follow-up measures and actions to be taken to improve the quality of the core products and services provided by EPO. Contact details of the target users, including name, company, telephone/fax number and e-mail address, if available, need to be extracted from EPO databases and processed in order to make the interviews possible.

All contact details extracted from EPO databases for the user satisfaction surveys are publicly available, e.g.
through the EPO register, with one exception:
• For the user satisfaction survey on search services, a part of the sampled applications may not have been published yet at the date of the interview carried out by the external processor. The contact details, including personal data, of said applications are therefore not yet publicly available. However, the EPO considers it relevant to have user feedback from recent searches. Disregarding unpublished applications would negatively affect the goal of the surveys, which is to gather user feedback on the current performance of the EPO.

Personal data may be part of the contact details included in the different samples of potential respondents that are transferred to the external processor conducting the interviews.

The EPO uses an initial external processor to transfer the samples to a second external processor. According to the first external processor, all transfers uploaded from the EU (as determined from the client IP address) will be stored on servers in the EU. The EPO encrypts and password-protects all files sent.

The second external processor has been appointed to conduct these surveys and produce statistical reports under the instructions of the EPO. Potential respondents (i.e. users having received/used EPO products and services before the survey) are contacted via e-mail and/or telephone and reply to the questions on a voluntary basis.

The second external processor uses the contact details received from the EPO to reach the potential respondents. These contact details, however, are not always sufficient. The second external processor complements the contact details with further information, sometimes including personal data, from their own databases (from former and current surveys), from the Internet (e.g. LinkedIn, webpages of the companies) or gathered during contacts with respondents through various communication channels such as phone calls, emails, etc. The responses are collected in order to perform statistical processing to explore cause-effect relationships related to satisfaction with the

Purpose of Processing The objective of this processing activity is to measure the level of users' satisfaction e.g. by type of user in order to identify the follow-up measures and actions to be taken to improve the quality of the core products and services provided by the EPO.

products and services covered by each particular survey. As a result of the processing, statistical reports are produced. These reports contain the answers in an anonymous and aggregated form, in a manner that does not allow individual responses to be identified. The reports are then made available to EPO top management and further staff involved in the analysis of the results.

Neither the EPO nor the external processors use the personal data for any other purpose than carrying out the survey and collecting, aggregating and further analysing the results thereof.

Data Retention Personal data will be kept only for the time needed to achieve the purposes for which it is processed. At the EPO, personal data will be kept until completion of a second cycle of user satisfaction surveys and the publication of its results, i.e. a maximum of 5 years. Personal data will then be deleted.

Regarding the first external processor, the uploaded file or files (the upload) through their website are stored on their servers for a period of 7 days by default, afterwards the upload is automatically deleted.

The second external processor keeps personal data for the whole duration of their contract with the EPO for further user surveys. According to this contract, the external processor shall, upon termination of the contract, either completely and irrevocably delete any EPO data or return back to the EPO all EPO data and storage media including any copies thereof, unless the external processor is obligated by applicable law to further store EPO data, in which case the contractor shall inform the EPO accordingly in writing. In the event of a formal appeal/litigation, all data held at the time the formal appeal/litigation was initiated will be retained until the proceedings have been closed.

Data subjects and categories of personal data

Externals

General	
Answers to surveys, assessments or quizzes	
Contact Information	
Contact Details	Country
Home Address	Phone Numbers
Working email address	
Employment Information	
Company Entity	
Personal Identification	
First Name	Full Name
Surname	

Recipient of the personal data

Recipients of the data Personal data are processed by the EPO staff involved in managing the User Satisfaction Survey (USS) programme.

The samples are transferred to the external processor BERENT Deutschland GmbH using the external processor WeTransfer.

BERENT Deutschland GmbH processes the personal data within its offices in Kassel (DE) and in Vilnius (LT).

Personal data are disclosed on a need-to-know basis to the EPO staff involved in managing the User Satisfaction Survey (USS) programme, e.g. manual checks in samples and could also be disclosed on a need-to-know basis to other EPO staff, e.g. to Directorate 53 (Patent Law & Procedures) in case of a complaint which needs their input.

Personal data will only be shared with authorised persons responsible for the necessary processing operations. They will not be used for any other purposes or disclosed to any other recipients.

Purpose of sharing The EPO uses external processor WeTransfer to transfer the samples to external processor BERENT Deutschland GmbH. According to the external processor WeTransfer, all transfers uploaded from the EU (as determined from the client IP address) will be stored on servers in the EU. The EPO encrypts and password-protects all files sent.

The external processor BERENT Deutschland GmbH has been appointed to conduct these surveys and produce statistical reports under the instructions of the EPO. Potential respondents (i.e. users having received/used EPO core products and services within the above specified period before the survey) are contacted via e-mail and/or telephone and reply to the questions in a voluntary basis. The external processor BERENT Deutschland GmbH uses the contact details received from the EPO to reach the potential respondents. Said contact details, however, are not always sufficient. The external processor BERENT Deutschland GmbH complements the contact details with further information, sometimes including personal data, from their own databases (from former and current surveys), from Internet (e.g. LinkedIn, webpages of the companies) or gathered during contacts with respondents through various communication channels such as phone calls, emails, etc. The responses are collected in order to perform statistical processing to explore cause-effect relationships related to satisfaction with the core products and services covered by each particular survey. As a result of the processing, statistical reports are produced. These reports contain the answers in an anonymous and aggregated form, in a manner that does not allow individual responses to be identified. The reports are then made available to EPO top management and further staff involved in the analysis of the results.

Transfer

Transfer No

Transfer to public authority and/or International Organisation No

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors) WeTransfer - Netherlands, BERENT Deutschland GmbH - Germany

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR The transfer is necessary for the performance of a task in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning, or to perform obligations arising from its duty of co-operation with the contracting states

Organisational and security measures

Organisational and security measures We take appropriate technical and organisational measures to safeguard and protect your personal data from accidental or unlawful destruction, loss or alteration and unauthorised disclosure or access. All personal data are stored in secure IT applications in accordance with the EPO's security standards. Appropriate levels of access are granted individually only to the above-mentioned recipients. User personal data are stored on systems located on EPO premises. EPO staff store and process user personal data according to the EPO Data Protection Rules (CA/D 5/21) and the EPO Information Security Guidelines (Circular 382 - Codex 1b). Regarding the transfer to the external processor BERENT Deutschland GmbH using the external processor WeTransfer, during an upload, while it's stored on the external processor WeTransfer's servers, and during a download, transfers are encrypted, password-protected and then sent over a secured connection (https) only. The external processor BERENT Deutschland GmbH is bound by confidentiality according to the terms of the contract. For systems hosted on EPO premises, the following basic security measures generally apply: • User authentication and access control (e.g. role-based access control to the systems and network, principles of need-to-know and least privilege) • Logical security hardening of systems, equipment and network • Physical protection: EPO access controls, additional access controls to datacentre, policies on locking offices • Transmission and input controls (e.g. audit logging, systems and network monitoring) • Security incident response: 24/7 monitoring for incidents, on-call security expert.

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 320

Name Mass email distribution list management

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG4 - 46 - CIO / BIT

External processors

Sword Technologies

External processors	
Name Sword Technologies	

Microsoft

External processors	
Name Microsoft	

SendInBlue

External processors	
Name SendInBlue	

Indra

External processors	
Name Indra	

Microsoft

External processors	
Name Microsoft	

SendInBlue

External processors	
Name SendInBlue	

Description of the processing

Description This record of processing activity relates to the management of the SendInBlue tool used for the dispatch of mass e-mails, covering the automated collection, use, storage, transfer and destruction of email addresses and site information used to target specific subparts of the organisation, as well as the manual addition of new records and the manual deletion of departing members.

More specifically:
The main use case relates to mass emails addressed internally to EPO colleagues, such as for example mass e-mails from any statutory or social body of the EPO (e.g. statutory body under Article 2 of the Service Regulations, Amicale). Based on approved business cases (for example site-specific mails), the sending area will use their associated authorised email address (shared mailboxes owned by the relevant area) to send their mass mail to the tool, which will first check that the sender is indeed authorised and then forward the mail to the associated distribution list. The distribution lists are associated per authorised sending email address. The tool automatically tracks the opt out.
• BIT is responsible for the implementation, setup and maintenance of the environment for sending the mass mails and the distribution lists for the above are periodically (generally twice a month) extracted from the EPO Phone book and uploaded to the SendInBlue tool by BIT. Recipients can unsubscribe by opting-out from these distribution lists.

A second use case relates to mass emails addressed by specific business areas of the Office to mailing lists including externals.
• In these cases, the business area would have to periodically provide an up-to-date distribution list to BIT for uploading into the tool, as this cannot be derived from the phone book. The specific business areas will also remain responsible for confirming the opt-in (consent) of recipients. The consent management, if any is necessary, is handled by the respective business unit.

For both use cases:
• The relevant business units sending the emails do not have access to the tool which is sending the mass emails. The units can just send a mass email to the tool which will forward it to the distribution list associated with an authorised sending email address of the unit.
• The units sending the emails remain responsible for the contents of their messages, including responsibility for any personal data potentially included in their messages.

Purpose of Processing Managing mass email distribution lists

Data Retention Data will be deleted upon departure of the staff member for EPO staff, young professionals, seconded national experts (data is kept in the system until departure in order to track in the system that the staff member has opted out). Externals, including members of the general public, who opt into a list and do not opt out, will be deleted upon decommissioning of the distribution list.

At the end of the contractual relationship, Sendinblue undertakes to destroy all personal data within a maximum period of three (3) months, subject to Sendinblue's requirements to store data for legal purposes.

Data subjects and categories of personal data

Contractors

Contact Information	
Contact Details	Country
Home Address	Phone Numbers
Working email address	
Correspondence	
Personal information provided voluntarily	
Browsing Information	
IP Address	
Employment Information	
Company Entity	Office Location
Personal Identification	
Full Name	
User Account Information	
User ID	

Employees

Contact Information	
Contact Details	Country
Home Address	Phone Numbers
Working email address	
Correspondence	
Personal information provided voluntarily	

Browsing Information	
IP Address	
Employment Information	
Company Entity	Office Location
Personal Identification	
Full Name	
User Account Information	
User ID	

Externals

Contact Information	
Phone Numbers	Working email address
Browsing Information	
IP Address	
Personal Identification	
Full Name	

Recipient of the personal data

Recipients of the data - BIT staff in charge of the email system belonging to SWORD, WAST, and PACE (BIT 4615)
- BIT subcontractors who administer the email system
- SendInBlue
- Microsoft
- Relevant business unit providing a distribution list

Purpose of sharing BIT staff and subcontractors in charge of the email system for the purpose of managing the service. Sendinblue processes personal data for purposes of provisioning the Service. Microsoft processes personal data by having the parties send the distribution lists and/or content of the email to be distributed through Microsoft tools (e.g. Outlook, Exchange Online)

Relevant business units providing a distribution list are informed when there are non-deliveries, in order for the business unit to clean-up their list. Typically non-deliveries occur when a wrong email address is provided or the recipient mailbox has been deleted in the meantime.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards, EC Adequacy Decision, Data Protection EU Comm Standard Contractual Clauses

Country where data might be transferred - Processor (Vendors) Microsoft - United States, SendInBlue - United States, SendInBlue - Canada

Reasons for the transfer Used by SendInBlue in order to ensure their services, via what is commonly known as a Content Delivery network (CDN), For Microsoft: protection against malware, login to Azure Active Directory, error analysis, load balancing, diagnostics data, connected experiences, and processing for Microsoft's business operations, Customer experience & Maintenance

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 345

Name Quantifying the user-specific usage of MyEPO Portfolio service and publishing the Top Digital Champions of the MyEPO Portfolio service on epo.org

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 45 - CTO / BIT, DG1 - 15 - Customer Journey and KAM

Entity Name - Controller (Entities) DG1 - 15 - Customer Journey and KAM

External processors

MongoDB UK Limited

External processors	
Name MongoDB UK Limited	

Description of the processing

Description This record explains how personal data are processed in order to establish a list of the Top Digital Champions for publication on the EPO website (epo.org).

This record also explains how the data are processed to identify users (i.e. companies, applicants or patent attorney firms) who use the MyEPO Portfolio services to quantify their usage of MyEPO Portfolio.

The Top Digital Champions of the MyEPO Portfolio service are determined by tracking MyEPO Portfolio usage metrics. The number of downloads of communications in the MyEPO Portfolio Mailbox is taken as basis for measuring usage metrics.

The number of downloads of communications in the MyEPO Portfolio Mailbox is counted on a rolling quarterly basis.

(https://bi4you.internal.epo.org/#/views/MyEPOAdoption/MailboxDashboard?:iid=1)

In addition, the numbers of the following types of replies to EPO communications via MyEPO Portfolio are counted:

• replies to communications under Rule 71(3) EPC about the intention to grant
• replies to communications from the examining division under Article 94(3) EPC
• responses to extended European search reports
• replies to invitations to clarify the subject-matter for search (CLAR)
• replies to PCT search reports

The companies or applicants with the highest number of such counts will appear in descending order in a publicly available list of Top Digital Champions on the EPO website in dependence on the user categories accessing the MyEPO Portfolio service (i.e. companies, applicants or patent attorney firms).

The processing is not intended to be used for any automated decision-making, including profiling.

Data Retention Personal data will be kept only for the time needed to achieve the purposes for which it is processed.
Personal data processed for this purpose will be deleted 5 years after the date of collection after their collection.
In the event of a formal appeal/litigation, all data held at the time the formal appeal/litigation was initiated will be retained until the proceedings have been closed.

Purpose of Processing The data are processed to establish a list of the Top Digital Champions for publication on the EPO website and to identify the user categories accessing the MyEPO Portfolio service (i.e. companies, applicants or patent attorney firms) and quantify usage metrics.

Data subjects and categories of personal data

Externals

Contact Information	
Country	
Device Management Data	
Account ID	
Employment Information	
Company Entity	
Personal Identification	

Full Name	

Recipient of the personal data

Recipients of the data Personal data are disclosed on a need-to-know basis to the EPO staff working in DG 1's PD 1.5 Customer Journey and Key Account Management and DG 4's PD 4.5 CTO, which is part of BIT.

Personal data will only be shared with authorised persons responsible for the necessary processing operations. They will not be used for any other purposes or disclosed to any other recipients.

Purpose of sharing Personal data are disclosed on a need-to-know basis to the EPO staff working in DG 1's PD 1.5 Customer Journey and Key Account Management and DG 4's PD 4.5 CTO, which is part of BIT.

Personal data will only be shared with authorised persons responsible for the necessary processing operations. They will not be used for any other purposes or disclosed to any other recipients.

The personal data are processed to establish a list of the Top Digital Champions for publication on the EPO website and to identify the user categories accessing the MyEPO Portfolio service (i.e. companies, applicants or patent attorney firms) and quantify usage metrics.

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 356

Name Communication sent and social activities organised for staff by Amicale Berlin

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 45 - CTO / BIT, DG4 - 46 - CIO / BIT

Entity Name - Controller (Entities) Chief Inter-Amicale Officer (CIAO)

External processors

Microsoft

External processors	
Name Microsoft	

SendInBlue

External processors	
Name SendInBlue	

Microsoft

External processors	
Name Microsoft	

SendInBlue

External processors

Name	
SendInBlue	

Description of the processing

Description Amicale Berlin processes personal data in the context of the organisation of activities (e.g. by collecting information via the online form published on Amicale Berlin website: http://www.amicale-berlin.org) and by sending general communication about Amicale's activities via email to all Berlin permanent staff under Article 1 ServRegs and/or contractors.

For activities organised exclusively by Amicale Berlin, any personal data collected will stay with the Amicale Berlin members and no personal data will be transferred to recipients outside the EPO. The processing is not intended to be used for any automated decision-making, including profiling.

Where a third party is involved in the organisation of an Amicale event, personal data may be provided to recipients outside the EPO to the extent that is necessary for the intended purpose.

Data Retention For Amicale Berlin activities, personal data will be deleted after the activity is over and all outstanding liabilities in relation to the event are settled.

With regards to the personal data processed for sending the communication, the relevant information on the applicable retention period can be found in Record No. 320 available in the EPO Data Protection Register.

Purpose of Processing Sending information to all Berlin permanent staff in under Article 1 Service Regulations and/or contractors, Registration to Amicale Berlin activities

Data subjects and categories of personal data

Contractors

Contact Information	
Contact Details	Personal Email
Working email address	
Personal Identification	
Age	First Name
Surname	

Employees

Contact Information	
Contact Details	Personal Email
Working email address	
Personal Identification	
Age	First Name

Surname	

Externals

Contact Information	
Contact Details	
Personal Identification	
Age	First Name
Surname	

Recipient of the personal data

Recipients of the data The internal and external processors.

Purpose of sharing The BIT department is responsible for the management of the tool used for the dispatch of the communication, including for the destruction of the email addresses and site information used to target the communications, whereas the tools are necessary to carry out the purpose of the processing.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards, Data Protection EU Comm Standard Contractual Clauses, EC Adequacy Decision

Country where data might be transferred - Processor (Vendors) Microsoft - United States, SendInBlue - United States, SendInBlue - Canada

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data

protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 358

Name Processing of personal data by the EPO Observatory on Patent and Technology

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 46 - CIO / BIT, DG0 - 03 - Corporate Governance Service

Entity Name - Controller (Entities) DG0 - 03 - Patent Research and Policies

Description of the processing

Description Personal Data are collected and processed for the purpose of creating a contact lists of stakeholders relevant for the activities carried out by the EPO Observatory on Patent and Technology in the Principal Directorate Patent Research and Policies, which is to develop and maintain a network of formal and informal contacts with international key players in the innovation ecosystems. Personal data will be gathered through an automated processing by completing an electronic form. The objective is to firstly map potential stakeholders and secondly to implement institutional or contractual relations necessary to develop the activities of the Observatory (agreements, call for expertise to participate in studies or events and/or financial compensations). The data will also be used for
- sending invitations to Observatory related events
- providing information on Observatory related activities
- organize surveys on activities related to the Observatory mission and activities
- build up a digital library of publications related to innovation which are publicly available, in which the author/owner/contributor/source could be mentioned.

Data Retention Personal data will be kept from collection only for the time needed to achieve the purposes for which they are processed.

The contacts database is updated regularly (at least twice a year) and stakeholders that are no longer relevant are removed. Data that have become obsolete are deleted from the contacts database.

Purpose of Processing Implement institutional or contractual relations necessary to develop the activities of the Observatory (agreements, call for expertise to participate in studies or events and/or financial compensations)., Organize surveys, Build up a digital library of publications related to innovation which are publicly available, in which the author/owner/contributor/source could be mentioned., Providing information on Observatory related activities, Develop and maintain a network of formal and informal contacts with international key players in the innovation ecosystems., Sending invitations to Observatory related events, map potential stakeholders

Data subjects and categories of personal data

Externals

General	
Answers to surveys, assessments or quizzes	
Contact Information	
Contact Details	Country
Mobile Phone Number	Personal Email
Phone Numbers	Working email address
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	
Professional Experience & Affiliations	
CV	
Employment Information	
Business Unit Division	Company Entity
Department name and/or number	Job Title Role
Language preference (of communication)	
Personal Identification	
First Name	Full Name
Surname	Nationality
Education & Skills	
Education and Training History	Educational Degrees
Languages	Project management experience
Technical expertise	

Recipient of the personal data

Recipients of the data The personal data are disclosed on a need-to-know basis to the EPO staff working in the Principal Directorate Patent Research and Policies with the aim to processing activities that are necessary for the EPO Observatory on Patent and Technology to fulfil its role. No external entity will have access to the data

Purpose of sharing The purpose of the sharing is to allow the perform the processing activities that are necessary for the EPO Observatory on Patent and Technology to fulfil its role, which is to develop and maintain a network of formal and informal contacts with international key players.

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer

Transfer mechanism(s)	Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network	

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 360

Name Personal data processing for insurance purposes and damage claim handling

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 44 - General Administration

Entity Name - Controller (Entities) DG4 - 44 - General Administration

External processors

Marsh GMBH

External processors	
Name Marsh GMBH	

Marsh GMBH

External processors	
Name Marsh GMBH	

Description of the processing

Description Personal data are required for the processing and settlement of damage claims. These data may be collected from EPO employees, contractors, and external parties. If video footage is deemed necessary, approval must be obtained from the PD 4.4 delegated controller, after which the security team from the Operations office will secure the footage. A joint review of the footage will be conducted by the security and Insurance teams.

The extent of damage coverage is verified against existing insurance contracts, which may require disclosing personal data to third parties, such as the insurance broker.

Purpose of Processing Personal data, date and time of damage as well as pictures / video footage needed to evaluate the insurance claim (process of damage) and file a single case decision.

Data Retention The data received via email or through the form in the mailbox are kept in outlook. Personal data are kept until final decision of damage claim and acceptance by all involved parties which can last on average between 3 to 9 months. 3 years after settlement of the claim they are deleted.

Data subjects and categories of personal data

Employees

Contact Information	
Phone Numbers	Working email address
Financial	
Insurance Information	
Travel & Expense	
Travel Booking Details	
Personal Identification	
Full Name	
Government Identifiers	
Car registration documents	

Externals

Contact Information	
Contact Details	
Financial	
Insurance Information	
Personal Identification	
Full Name	

Contractors

Contact Information	
Phone Numbers	Working email address
Financial	
Insurance Information	
Personal Identification	
Full Name	

Government Identifiers	
Driving Licence Number	

Recipient of the personal data

Recipients of the data EPO internally: potentially staff members working in teams Operation Office (for Security) and Building maintenance depending on damage area, and the safety officer.

Finance department in case of reimbursement (special cases) to EPO staff

EPO externally: EPO's insurance broker Marsh, contracted insurer, e.g. liability insurer AXA

Purpose of sharing Personal data are shared to handle damage claims.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation The data sharing is a Controller to controller relationship and this is considered a transfer of personal data under Articles 8(5) and 9 DPR.

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors) Marsh GMBH - Germany

Reasons for the transfer For damage claim handling purpose

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, All necessary personal data are collected based on the need of individual damage claim handling, per case. DPO is contacted for every individual case, if video footage deemed necessary for decision taking and data is to be secured. Insurance broker Marsh contractually confirmed confidentiality in handling with personal data (broker contract point 6) and confirmed data protection and privacy principles (broker contract point 11)

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 362

Name External general tasks and activities carried out by PD02

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 46 - CIO / BIT, DG4 - 45 - CTO / BIT

Entity Name - Controller (Entities) DG0 - 02 - Communication

External processors

OpenText

External processors	
Name OpenText	

Spatial Chat

External processors	
Name Spatial Chat	

Bitly

External processors	
Name Bitly	

Huddle

External processors

Name	
Huddle	

Microsoft

External processors	
Name	
Microsoft	

Description of the processing

Description The scope of the activities of PD Communication and the processing of personal data necessary to carry out theses activities are aligned with its organisational structure and includes the following: The processing of personal data in the context of creating and distributing communication materials involves the collection and use of contact information and, in some cases, feedback from internal and external stakeholders. This data may be used to tailor content such as newsletters, landing pages, or social media posts to relevant audiences, and to improve communication strategies. The processing is partially automated, as it involves the use of digital tools and platforms (e.g. content management systems, design software, databases, email marketing tools) to draft, produce, and distribute content, while some aspects (e.g. drafting, strategic planning) may still involve manual input.

Similarly, the management of communication channels includes the distribution of announcements and messages via electronic means such as email services. This involves automated processing of personal data, including email addresses and potentially names or job titles, especially when targeting specific audiences based on predefined business cases. Requests to use the EPO Mail Service are handled in coordination with relevant business units or statutory bodies, and the communication process relies on structured electronic systems to ensure efficient and accurate delivery.

Data Retention Personal data will be kept only for the time needed to achieve the purposes for which it is processed.

For surveys and consultations, personal data will be deleted in a maximum of three (3) years after the end of the user consultation.

Personal data used in the framework of the emailing service that PD Communication provides will be automatically deleted from the EPO Mail Service upon departure of the EPO employee from the Office, or upon request of the data subject to the relevant unit, if applicable. Personal data stored in the PD Communication's dedicated request register are deleted after 3 years upon receipt of the request.

In the event of a formal appeal/litigation, all data held at the time the formal appeal/litigation was initiated will be retained until the proceedings have been closed.

Purpose of Processing Creation and Distribution of communication materials:, Management of communication channels:

Data subjects and categories of personal data

Employees

Matter/Log file	
Attachments	Metadata

General	
Answers to surveys, assessments or quizzes	Any other information
Multimedia material	
Contact Information	
Contact Details	Working email address
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Feedback received
Personal information provided voluntarily	
Personal Identification	
First Name	Full Name
Gender	Surname
Picture	
Education & Skills	
Languages	

Externals

General	
Answers to surveys, assessments or quizzes	Any other information
Multimedia material	
Contact Information	
Mobile Phone Number	Personal Email
Working email address	
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	
Correspondence	

Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Employment Information	
Membership in a EPO Staff Committee	
Personal Identification	
First Name	Full Name
Surname	

Former Employees

General	
Answers to surveys, assessments or quizzes	Multimedia material
Contact Information	
Personal Email	
Personal Identification	
First Name	Full Name
Surname	

Recipient of the personal data

Recipients of the data

Personal data will only be shared with authorised persons responsible for the necessary processing operations. They will not be used for any other purposes or disclosed to any other recipients.

A limited number of EPO employees in different departments of the EPO (e.g.: Principal Directorate Communication, Principal Directorate People, Business Information Technology, Principal Directorate General Administration, President's Office and Vice-President DGs 1, 4 and 5) have access to the personal data collected, on a need-to-know basis.

For instance, in reference to the mass notification service to manage crisis control, please be informed that in actual emergency scenarios, the notifications will be sent by PD Communication under the supervision of the President/President's deputy.

Purpose of sharing

As for surveys and consultations, any other data shared as part of the results of the consultation will be displayed in anonymous form.

Personal data may be disclosed to third-party service providers for maintenance and support purposes. It may be also disclosed to third-party service providers for the purpose of providing a consultation platform and tools for the processing of results.

When publishing content on the internal and external channels of the EPO in order to carry out any of the activities mentioned in point 1 of this data protection statement that refers to the purpose of promoting or communicating the EPO image and activities, personal data may be shared with the public having access or using those channels.

Transfer

Transfer No

Country where data might be transferred - Processor (Vendors)
Huddle - United Kingdom, Microsoft - United States, OpenText - United Kingdom

Transfer to public authority and/or International Organisation

Reasons for the transfer

Transfer mechanism(s)

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted on EPO premises, most of the external providers supporting the EPO generally commit in a binding agreement to comply with their data protection obligations under the applicable data protection legal frameworks. The EPO has also carried out a privacy and security risk assessment. These systems are required to have implemented appropriate technical and organisational measures such as: physical security measures, access and storage control measures, securing data at rest (e.g., by encryption); user, transmission and input control measures (e.g., network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), audit logging); conveyance control measures (e.g., securing data in transit by encryption).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 365

Name User Consultation 2023 - amendments RPBA

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) BoA - Deputy of the President of the Boards of Appeal, BoA - The President of the Boards of Appeal

Entity Name - Controller (Entities) DG5 - 501 - Council Secretariat

Description of the processing

Description The BOAC and the PBoA conduct a user consultation on proposed amendments to the Rules of Procedure of the Boards of Appeal. A user consultation is conducted in order to obtain feedback from users on the proposed amendments to the Rules of Procedure of the Boards of Appeal. Personal data are processed for the purpose of obtaining knowledge of the users' views on the proposed amendments. This may lead to a refinement of the proposed amendments.

Data Retention Data will be kept for a maximum period of 10 years after the conclusion of the user consultation.

Purpose of Processing Obtaining knowledge of the users' views on the proposed amendments is of key importance to refine them.

Data subjects and categories of personal data

Externals

General	
Answers to surveys, assessments or quizzes	Legal opinions and assessments
Contact Information	
Contact Details	Phone Numbers
Working email address	
Professional Experience & Affiliations	
Affiliation	

Representation in EPO's Patent Granting Process	
Affiliation to Association of professional representatives	
Personal Identification	
First Name	Full Name
Surname	

Recipient of the personal data

Recipients of the data BOAC members and alternate members will have access to the data, as well as the President of the Boards of Appeal and a limited number of staff members of the EPO, in particular of the Boards of Appeal (e.g.: the Head of the Legal Services of the Boards of Appeal, staff members of the Legal Advice Service of the Boards of Appeal) of the Council Secretariat, as well representatives of the President of the European Patent Office, who has the opportunity to provide comments to amendments to the RPBA (see R. 12c(2) EPC) have access to the personal data collected in the user consultation, on a need-to-know basis. Any other data shared as part of the results of the consultation will be displayed in anonymous form.
Personal data will only be shared with authorised persons responsible for the necessary processing operations.
They will not be used for any other purposes or disclosed to any other parties.

Purpose of sharing Data will be shared with colleagues involved in the enactment of the amendments to the Rules of Procedure of the Boards of Appeal

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 368

Name “EPO Contingency Upload Service” for the parties to proceedings before the EPO (PGP)

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG1 - 11 - COO, DG4 - 45 - CTO / BIT

Entity Name - Controller (Entities) DG1 - 15 - Customer Journey and KAM, DG1 - 1 - Patent Granting Process

External processors

Google Ireland Limited

External processors	
Name Google Ireland Limited	

Description of the processing

Description The EPO Contingency Upload Service (CUS) is a tool to be used in exceptional cases of emergency, where the existing filing solutions are not available to external users. It enables users to upload one or more documents and receive a confirmation from the EPO that these documents have been received and stored securely, together with the timestamp of this receipt.

Personal data is processed for the purposes of the EPO CUS when uploading documents related to the patent-grant and proceedings (PGP) pursuant to the EPC and the provisions applicable under it, and likewise proceedings under the Patent Cooperation Treaty (PCT) and the Unitary Patent Rules (UPR).

Personal data is collected when users upload one or more documents in the Contingency Upload Service. The uploaded data are encrypted and stored securely on infrastructure operated by the EPO and hosted on the EPO's cloud service provider (google cloud platform).

Personal data are used to identify the user performing an upload and/or any other party that is signing the uploaded package. Frequently, submissions are signed by a different person than the one logged into the system. Therefore, in CUS (as part of each upload) the EPO asks the user to fill in the information of the signing party and a text string signature corresponding to the name of the signing party.

The personal data are also processed using the PGP back-office systems allowing EPO staff to process patent applications and any other subsequently filed document, pursuant to the EPC, the PCT and the the provisions applicable under them.

The processing is not intended to be used for any automated decision-making, including profiling.

Personal data will not be transferred to recipients outside the EPO which are not covered by Article 8(1), (2) and (5) DPR unless an adequate level of protection is ensured. In the absence of an adequate level of protection, a transfer can only take place if appropriate safeguards have been put in place and enforceable data subject rights and effective legal remedies for data subjects are available, or if derogations for specific situations as per Article 10 DPR apply.

Data Retention A patent provides a legal protection for 20 years, and there is no limitation to how long the post-grant procedures can last: after the patent granting procedure, there can be an opposition procedure which will review the patent granting procedure and involve members of the examining division. These members need to be able to retrieve their actions and comments. Moreover, after the patent granting procedure, there can be an appeal procedure whose outcome can be to reopen the examination procedure by the examining division. After that, revocation and limitation procedures may take place at any time, even after expiry of the patent protection. The examining division needs to be able to retrieve the actions and comments of the initial procedure. For more information, see the Decision of the President of the European Patent Office dated 13 December 2021 concerning the processing of personal data in patent-grant and related proceedings (OJ EPO 2021 A98). Personal data used which is part of the patent grant procedure is stored indefinitely. If considered appropriate, other personal data (for example names of administrative staff of a representative that process uploads performed via the EPO Contingency Upload Service) can be deleted if it can reasonably be expected that there is no operational need anymore, with a maximum of 10 years. In the event of a formal appeal/litigation, all data held at the time the formal appeal/litigation was initiated will be retained until the proceedings have been closed.

Purpose of Processing The EPO Contingency Upload Service (CUS) is a tool to be used in exceptional cases of emergency, where the existing filing solutions are not available to external users. It enables users to upload one or more documents and receive a confirmation from the EPO that these documents have been received and stored securely, together with the timestamp of this reception.

Data subjects and categories of personal data

Externals

Contact Information	
Contact Details	Country
Home Address	Mobile Phone Number
Personal Email	Phone Numbers
Private Phone Number	Working email address
European Patent Register Data	
Address	
Representation in EPO's Patent Granting Process	
Affiliation to Association of professional representatives	
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	
Financial	
Bank Account Information	Credit Card Number
Debit Card Number	
Employment Information	
Company Entity	Corporate Credit or Debit Card Numbers
Department name and/or number	Job Title Role
Office Location	
Personal Identification	
First Name	Full Name
Surname	Signature
Government Identifiers	
National Identity Card Details	Passport Number

Recipient of the personal data

Recipients of the data Personal data are processed under the responsibility of DG 1's PD 15 Customer Journey and Key Account Management, acting as the EPO's delegated data controller.

Personal data are processed by the EPO staff in departments 1195 (Classification Support, File Management, SCAPES and CDR) and 45331 (Front Office Tools) responsible for operating the EPO Contingency Upload Service.

DG 4 staff and external contractors involved in maintaining the EPO Contingency Upload Service may also process or have access to personal data.

Purpose of sharing Operating the EPO Contingency Upload Service referred to in this statement.
Maintaining the EPO Contingency Upload Service.

Transfer

Transfer No

Country where data might be transferred - Processor (Vendors)
Google Ireland Limited - Hong Kong, Google Ireland Limited - Taiwan, Google Ireland Limited - Brazil, Google Ireland Limited - Qatar, Google Ireland Limited - Indonesia, Google Ireland Limited - Singapore, Google Ireland Limited - Malaysia, Google Ireland Limited - Saudi Arabia, Google Ireland Limited - United States, Google Ireland Limited - Philippines, Google Ireland Limited - India, Google Ireland Limited - Australia, Google Ireland Limited - Chile

Transfer to public authority and/or International Organisation

Reasons for the transfer

Transfer mechanism(s)

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums)., We take appropriate technical and organisational measures to safeguard and protect your personal data from accidental or unlawful destruction, loss or alteration and unauthorised disclosure or access. All personal data are processed and stored in secure IT applications in accordance with the EPO's security standards. These include: • User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. • Access control (e.g. role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. • Logical security hardening of systems, equipment and network. • Physical protection: EPO access controls, additional access controls to datacentre, policies on locking offices. • Transmission and input controls (e.g. audit logging, systems and network monitoring). • Security incident response: 24/7 monitoring for incidents, on-call security expert. Appropriate levels of access are granted individually only to the abovementioned recipients. As a contingency service, EPO CUS is hosted on EPO's cloud service provider (Google Cloud Platform). The EPO cloud service provider has committed in a binding agreement to comply with their data protection obligations under the applicable data protection legal frameworks. The EPO has also carried out a privacy and security risk assessment. These systems are required to have implemented appropriate technical and organisational measures such as: physical security measures, access and storage control measures, securing data at rest (e.g. by encryption); user, transmission and input control measures (e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), audit logging); conveyance control measures (e.g. securing data in transit by encryption). On top of the standard security measures implemented by the EPO cloud service provider, the following measures have been specifically implemented for the Contingency Upload Service: The upload package (I.e. the documents included in an upload) are zipped and encrypted with AES-256 encryption algorithm. A different encryption key is generated for each upload package. The encrypted upload package is stored on the file store.

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 376

Name Activities organised by Amicale Munich

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) Chief Inter-Amicale Officer (CIAO)

External processors

Microsoft

External processors	
Name Microsoft	

COMU GmbH

External processors	
Name COMU GmbH	

Microsoft

External processors	
Name Microsoft	

Description of the processing

Description The Amicale Munich processes personal data as follows:

• Registration: Amicale Munich collects personal data via registration forms published on the Amicale Munich dedicated website.
To register for an activity, attendees are requested to provide first and last names and email.

In the case of children, if any, the age range of the children (adapted for the particular needs, e.g. toddlers <6, children <12, youths <18, adults 18+) are processed. This is for instance the case for ski weekends with hotel bookings and ski pass purchases.

• Payment: for specific activities where a fee is requested, Amicale Munich collects bank details of the Amicale members and provides them to the bank for executing the direct debit payments. Should the payment do not work, Amicale Munich checks with the concerned Amicale member the reasons and process the data to collect the missing payments.

• Multimedia material: during the event, multimedia material might be produced (e.g. pictures) and used for communication purposes, e.g. being published on the Amicale Munich website and/or the EPO intranet.

• Attendees' lists: Amicale Munich keeps a list of the attendees and information on the payments until outstanding liabilities in relation to the event are settled, and for the purpose of including accurate figures in the annual report.

• Amicale Munich website: the Amicale Munich website includes a contact form to contact Amicale Munich, as well as the full names of the Amicale Clubs' members.
The Amicale Munich website is not publicly accessible, it can only be accessed if the data subject connects via the EPO VPN or has been granted by Amicale Munich with credentials (this is usually the case for EPO pensioners). General information regarding the processing of personal data carried out by Amicale Munich is included on the dedicated website.

• Clubs' annual subsidies: for clubs' annual subsidies, Amicale Munich requests from the Clubs the list of EPO staff members. This is done for the purpose of reporting, in particular the figures of EPO staff members' participation in the Clubs' activities, by means of the annual reports. This information is provided by email to the Amicale Munich committee and are deleted from the Amicale Munich drives every year after the annual meeting.

• Grants for holiday camps for kids children's camps: for the payment of subsidies, Amicale Munich receives via email a list from the external service providers with the names of the registrants, their EPO e-mail address and the number and age of the children registered.

• Annual reports: Amicale Munich publishes yearly an official report about its activities and finances. The only personal data included in the report are, in principle, the names of the Amicale elected committee.

• General assemblies: As soon as possible in the first quarter of each year, Amile Munich holds an annual general meeting ("AGM") to report to EPO Munich staff.

The agenda for the AGM includes the following items: (a) an activities report from the committee (b) a financial report from the treasurer (c) subsidies for clubs (d) the election of auditors (e) discharge of the committee (f) motions (g) any other business (h) if necessary, the appointment of an election committee under the election rules (see annex 1 of the Amicale Munich statutes).

• Elections: Elections are held every 2 years according to the election's rules (see annex 1 of the Amicale Munich statutes).

Purpose of Processing Organisation of the Amicale Munich activities, including registration and sending the necessary communications concerning the events. Distributing subsidies for Clubs according to the number of members. Payment of subsidies for participation in children's holiday programmes. Drafting and publishing an accurate annual report. Answering the queries received via the contact form. General communication purposes.

Data Retention Amicale Munich will delete all personal data after the activity is over, all outstanding liabilities in relation to the activities are settled, and the annual report is finalised.

Personal data used for the Payment of subsidies are deleted every year after the Annual General Meeting.

In the event of a formal appeal/litigation, all data held at the time the formal appeal/litigation was initiated will be retained until the proceedings have been closed.

Data subjects and categories of personal data

Externals

General	
Attendees' lists	List of Amicale Clubs' members
Multimedia material	
Contact Information	
Personal Email	
Financial	
Bank details	
Personal Identification	
Age	First Name
Surname	

Contractors

General	
Attendees' lists	List of Amicale Clubs' members
Multimedia material	
Contact Information	
Personal Email	Working email address
Correspondence	
Personal information provided voluntarily	
Financial	
Bank details	
Personal Identification	
First Name	Surname

Employees

General	
Attendees' lists	List of Amicale Clubs' members
Multimedia material	
Contact Information	
Personal Email	Working email address
Correspondence	
Personal information provided voluntarily	
Financial	
Bank details	
Personal Identification	
First Name	Surname

Former Employees

General	
Attendees' lists	List of Amicale Clubs' members
Multimedia material	
Contact Information	
Personal Email	
Correspondence	
Personal information provided voluntarily	
Financial	
Bank details	
Personal Identification	
First Name	Surname

Recipient of the personal data

Recipients of the data EPO staff working in the Amicale Munich and Kids committee (on a need-to-know basis), the EPO employees with access to the Amicale Munich website, and the bank to whom data subjects make the payment for certain activities.

Purpose of sharing Personal data will only be shared with authorised persons responsible for the necessary processing operations. They will not be used for any other purposes or disclosed to any other recipients. Personal data may be disclosed to third-party service providers for maintenance and support purposes.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards, Data Protection EU Comm Standard Contractual Clauses, EC Adequacy Decision

Country where data might be transferred - Processor (Vendors) Microsoft - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures For personal data processed on systems not hosted on EPO premises, the providers processing the personal data have committed in a binding agreement to comply with their data protection obligations under the applicable data protection legal frameworks. The EPO has also carried out a privacy and security risk assessment. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measure * Access and control measures: role-based principles of need-to-know and least privilege. * Securing data at rest e.g. by encryption, secure disposal of data carriers * User, transmission and input control measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), audit logging * Conveyance control measures e.g. securing data in transit by encryption, For systems hosted on EPO premises, the following basic security measures generally apply: * User authentication and access control e.g. role-based access control to the systems and network, principles of need-to-know and least privilege * Logical security hardening of systems, equipment and network * Physical protection: EPO access controls, additional access controls to datacentre, policies on locking offices * Transmission and input controls e.g. audit logging, systems and network monitoring * Security incident response: 24/7 monitoring for incidents, on-call security expert.

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 377

Name Activities organised by Amicale Vienna

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) Chief Inter-Amicale Officer (CIAO)

External processors

Microsoft

External processors	
Name Microsoft	

Domainfactory GmbH

External processors	
Name Domainfactory GmbH	

Polyas GmbH

External processors	
Name Polyas GmbH	

Microsoft

External processors	
Name Microsoft	

Description of the processing

Description Amicale Vienna processes personal data in the context of the organisation of social activities for EPO staff members, their families as well as externals (individuals requesting access to the Amicale Vienna website) ("data subjects").

Amicale Vienna collects personal data via registration forms published on the website.

To register for an event, attendees are requested to provide first and last names and email addresses. In the case of children, no personal data are collected but attendees shall indicate the No. of children and the age range (e.g. <6, <12).

During the event, multimedia material might be produced (e.g. pictures may be taken) and used for communication purposes, e.g. being published on the Amicale Vienna website and/or the EPO intranet.

Data subjects are informed about the possibility of multimedia material production via a disclaimer published on the Amicale Vienna website which is visible when registering for the events.

It should be noted that data subjects are free to exercise their right to object in a facilitated manner during the events (i.e. in case they do not wish to appear in a multimedia material they are free to not join the pictures or recordings and/or request the organiser of the particular event to not include them)

It should equally be noted that parents of the children are made aware of the risk related to the kids' exposure to the online environment.

For specific events where a fee is requested, Amicale Vienna provides attendees with the credentials of a bank account to receive the payment.

Amicale Vienna keeps a list of the attendees and information on the payments until outstanding liabilities in relation to the event are settled.

The Amicale Vienna website includes a contact form to contact Amicale Vienna and a "Small ads" space where members can post announcements on e.g. car sales, apartment to rent.

The website is not publicly accessible, it can only be accessible if the data subject connects via the EPO VPN or has been granted by Amical Vienna with credentials, this is usually the case for externals, i.e EPO pensioners.

Furthermore, the Amicale Vienna organises their elections, which are held every 2 years according to the election's rules

Data Retention For Amicale Vienna events, personal data will be deleted after the event is over and all outstanding liabilities in relation to the event are settled.

Purpose of Processing Organisation of the elections, • Organisation of the Amicale Vienna events, including registration and sending the necessary communications concerning the events • Answer the queries received via the contact form • Communications purposes • Publishing the "Small ads"

Data subjects and categories of personal data

Externals

General	
Content of small ads	Multimedia material
Contact Information	

Personal Email	
Correspondence	
Personal information provided voluntarily	
Personal Identification	
Age	First Name
Surname	

Contractors

General	
Content of small ads	Multimedia material
Contact Information	
Personal Email	Working email address
Correspondence	
Personal information provided voluntarily	
Personal Identification	
First Name	Surname

Employees

General	
Content of small ads	Multimedia material
Contact Information	
Personal Email	Working email address
Correspondence	
Personal information provided voluntarily	
Personal Identification	
Digital signature	First Name
Surname	Signature

Former Employees

General	
Content of small ads	Multimedia material

Contact Information	
Personal Email	
Correspondence	
Personal information provided voluntarily	
Personal Identification	
First Name	Surname

Recipient of the personal data

Recipients of the data Users with access to the Amicale Vienna website, as well as the internal and external processors, as necessary.

Purpose of sharing Users with access to the Amicale Vienna website, as well as the internal and external processors, as necessary.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards, Data Protection EU Comm Standard Contractual Clauses, EC Adequacy Decision

Country where data might be transferred - Processor (Vendors) Microsoft - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 378

Name Activities organised by Amicale the Hague

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) Chief Inter-Amicale Officer (CIAO)

External processors

Combell B.V.

External processors	
Name Combell B.V.	

Microsoft

External processors	
Name Microsoft	

Microsoft

External processors	
Name Microsoft	

Description of the processing

Description Amicale the Hague processes personal data in the context of the organisation of social activities for EPO staff members, their families as well as contractors and EPO pensioners ("data subjects").

Registration: Amicale the Hague collects personal data via registration forms published on the Amicale the Hague dedicated website.

To register for an activity, attendees are requested to provide first and last names and email addresses. In the case of children, depending on the activity, their first names are collected in agreement with a parent or legal guardian.. In addition, attendees are requested to indicate the No. of children and the age range (e.g. <6, <12).

Payment: for specific activities where a fee is requested, Amicale the Hague provides attendees with the credentials of a bank account (IBAN) to receive the payment. At a later stage, Amicale the Hague double-checks whether payment has been carried out, as information regarding the registered attendees and who paid is available to them and contact attendees when needed if they forgot to pay.

Multimedia material: during the event, multimedia material might be produced (e.g. pictures) and used for communication purposes, e.g. being published on the Amicale the Hague website and/or the EPO intranet.

Attendees' lists: Amicale the Hague keeps a list of the attendees and information on the payments until outstanding liabilities in relation to the event are settled, and for the purpose of including accurate figures in the annual report.

Amicale the Hague website: the Amicale the Hague website includes a contact form to contact Amicale the Hague.

The Amicale the Hague website is not publicly accessible, it can only be accessed if the data subject connects via the EPO VPN or has been granted by Amicale the Hague with credentials (this is usually the case for EPO pensioners). General information regarding the processing of personal data carried out by Amicale the Hague is included in the dedicated website.

Club's annual subsidies: for club's annual subsidies, Amicale the Hague requests from the Clubs the list of EPO staff members. This is done for the purpose of reporting, in particular the figures of EPO staff members' participation in the Clubs activities, by the means of the annual reports. This information is provided by email to the Amicale the Hague committee and are deleted from the Amicale the Hague drives every year after the annual meeting.

Annual reports: Amicale the Hague publishes yearly an official report about its activities and finances. The only personal data included in the report are, in principle, the names of the Amicale elected committee.

General assemblies: All EPO employees in the Hague are invited to the Amicale the Hague general assemblies. This invitation is sent out via mass e-mail, which is covered by dedicated data protection documentation. No personal data other than that of the Amicale the Hague committee are shared during the general assemblies.

Elections: The Amicale the Hague elections are either done during the general assemblies by raise of hands or by paper ballot. In the case of paper ballots, Amicale the Hague collects the names of the colleagues who voted for the exclusive purpose of avoiding double votes. This paper list is disposed of after the election.

Purpose of Processing • Organisation of the Amicale the Hague activities, including registration and sending the necessary communications concerning the events • Distributing subsidies for Clubs according to the number of members • Drafting and publishing an accurate annual report • Answer the queries received via the contact form • Communication purposes • Organising Amicale the Hague general assemblies • Organising Amicale the Hague elections

Data Retention Amicale the Hague will delete all personal data be deleted after the activity (including the elections) is over, all outstanding liabilities in relation to the activities are settled, and the annual report is finalised.

Data subjects and categories of personal data

Externals

General	
Attendees' lists	List of Amicale Clubs' members
Multimedia material	
Contact Information	
Personal Email	
Correspondence	
Personal information provided voluntarily	
Personal Identification	
Age	First Name
Surname	

Contractors

General	
Attendees' lists	List of Amicale Clubs' members
Multimedia material	Votes
Contact Information	
Personal Email	Working email address
Correspondence	
Personal information provided voluntarily	
Personal Identification	
First Name	Surname

Employees

General	
Attendees' lists	List of Amicale Clubs' members
Multimedia material	Votes

Contact Information	
Personal Email	Working email address
Correspondence	
Personal information provided voluntarily	
Personal Identification	
First Name	Surname

Former Employees

General	
Attendees' lists	List of Amicale Clubs' members
Multimedia material	
Contact Information	
Personal Email	
Correspondence	
Personal information provided voluntarily	
Personal Identification	
First Name	Surname

Recipient of the personal data

Recipients of the data Users with access to the Amicale the Hague website, as well as processors, as necessary.

Purpose of sharing Users with access to the Amicale the Hague website, as well as processors, as necessary.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards, Data Protection EU Comm Standard Contractual Clauses, EC Adequacy Decision

Country where data might be transferred - Processor (Vendors) Microsoft - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 383

Name Management of the MICADO Address Book (MAB)

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG5 - 501 - Council Secretariat

External processors

Zoom

External processors	
Name Zoom	

Microsoft

External processors	
Name Microsoft	

OpenText

External processors	
Name OpenText	

Microsoft

External processors	
Name Microsoft	

Zoom

External processors	
Name Zoom	

Description of the processing

Description MICADO Address Book (MAB): The CS collects, records, stores and updates personal data of selected EPO employees, delegates of member and observer states, non- governmental organisations, intergovernmental organisations, and external consultants participating in Administrative Council meetings in a dedicated database called MICADO Address Book (MAB).
MAB is accessible in MICADO which is a database managed by the Council Secretariat (CS). To access the MICADO database, user accounts are created for external users and need to be approved by the CS. MICADO users have access (read-only) to the MAB. EPO employees need to request MAB access to CS separately.
CS performs mainly the following actions:
(1) Collection: Personal data are usually provided by the data subject, notably members of a Council body, when announcing their participation to a meeting. The remainder is provided upon request by CS. MAB includes single records that can be printed, extracted and sorted in a preferred way and are constantly updated.
(2) Deactivation: Due to the changes in a delegation's composition (e.g. retirement, delegate no longer forming part of their delegation), the CS deactivates the access rights to MAB (see following paragraph) and set the record as non-public. In this case, these records are only accessible by the CS. The accounts of the EPO employees are deactivated automatically at the end of their service and hence will not be able to access MAB.

Data Retention A. Authorised MICADO Documents users (notably this group includes delegates): They are deleted upon request by the data subject. Otherwise they are marked as non-public and therefore are not visible to other users, but they remain accessible to the CS as long as such data can be needed e.g. in the process of finding suitable candidates for certain Committees' positions. EPO employees' data are deleted in MAB after they leave the Office. If a former EPO employee becomes a member in a Council's body after retirement (a rare occurrence) a new record will be created then.
B- External experts and consultants: personal data are kept as long as obligations by the Office exist including adequate time to check the fulfilment of those obligations.
C- Members of the Board of auditors and its experts: personal data are kept as long as obligations by the Office exist, including adequate time to check the fulfilment of those obligations.

Purpose of Processing Personal data are processed to ensure the organisation, administration and running of Council business; to keep historical record on composition of Council bodies; to fulfil contractual obligations of the European Patent Organisation towards council experts.

Data subjects and categories of personal data

Employees

Contact Information	
Contact Details	Country
MICADO ID user number	Mobile Phone Number
Phone Numbers	Working email address
Correspondence	

Personal information provided voluntarily	
Employment Information	
Department name and/or number	Duration of employment
End Date	Job Title Role
Language preference (of communication)	Office Location
Start Date	
Personal Identification	
First Name	Gender
Surname	Nationality
Picture	

Externals

Contact Information	
Contact Details	Country
MICADO ID user number	Mobile Phone Number
Phone Numbers	Working email address
Correspondence	
Personal information provided voluntarily	
Employment Information	
Department name and/or number	Duration of employment
End Date	Job Title Role
Language preference (of communication)	Office Location
Personal Identification	
First Name	Full Name
Gender	Surname
Nationality	Picture

Recipient of the personal data

Recipients of the data The members of Council bodies having MICADO Documents access have access to personal data which are defined as public: Member state, preferred language, last name, first name, postal address of the employer, email address and phone numbers. Participation and a role of a member in the Council's bodies is also visible as far as defined in MAB.

All other private information as well as records of the EPO employees and inactive records can be seen only by MAB administrators (i.e. D501 staff having full access rights to MAB and being able to add, change and delete records).

Personal data depending on its type and the purpose of its processing is made accessible on a need-to-know basis to Heads of delegation and their alternates (Council), Board of Auditors, and the external providers/their sub-contractors.

Directorate General DG 5, President's Office, upon request following approval by the Head of the Council Secretariat after assessment of the business case may have access to certain public parts of the information stored on the contact details database on a need-to-know basis.

External processors

Data published online (MICADO-P and EPO website) will be accessible by the general public.

Purpose of sharing See 1.16

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards, Data Protection EU Comm Standard Contractual Clauses

Country where data might be transferred - Processor (Vendors) Zoom - United States, OpenText - United Kingdom, Microsoft - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 386

Name Archiving of Council Secretariat's documents which include personal data

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG5 - 501 - Council Secretariat

External processors

SAP

External processors	
Name SAP	

OpenText

External processors	
Name OpenText	

Rhenus Office System GmbH

External processors	
Name Rhenus Office System GmbH	

Microsoft

External processors

Name
Microsoft

Description of the processing

Description Since 2010 the Council Secretariat has - for historical purposes - performed the following actions for the records of different nature and scope which are archived for administrative, institutional, legal and historical purpose. Personal data might be processed by the Council Secretariat when archiving CS's documents due to such activities:
1. index, catalogue, scan, and upload all CA and CA/C documents to the dedicated MICADO Documents and MICADO-C databases. These are repositories for the Council's documents managed by D501, while MICADO-C contains only the Council's confidential documents.
2. Index, catalogue and store Chairpersons and delegations' paper correspondence.
3. Index, catalogue and store confidential litigation records in respect of decisions of the AC as appointing authority: these are confidential paper records related to internal appeals and to disciplinary cases.
4. Index, catalogue and store (paper) records related to the drafting, approval and publication of CA documents.
5. store administrative documents (travel sheets and reimbursement to delegates and experts).

Data Retention A regular review will be conducted by the Council Secretariat and the retention policy adjusted as needed.

1. paper copies of the records uploaded on the dedicated MICADO Documents and MICADO-C document databases: one paper copy is sent to the external archives. The retention policy is
a) indefinite for the pre-1996 documents on MICADO, since the printed copies are considered the reference documents;
b) considered for disposal. Stored copies would be considered for disposal after 1996, since the versions uploaded on MICADO have been the reference documents.
2. Indefinite: Chairpersons and delegations' correspondence are kept indefinitely because of their historical value. This collection represents a mix of information of different memorial importance and confidentiality".
3. 15 years after pronouncement of appeal decision/ after lodging the appeal. Confidential Litigation records in respect of decisions of the AC as appointing authority.
4. Destruction after 3 years: paper related to drafting and processing ("common logs") for CA documents are destroyed 3 years after documents production. The older than 3 year archived documents are destroyed, and new documents will be destroyed after 3 years.
5. 3 years/3 months: Administrative documents (travel sheets and reimbursement). The archived documents older than 3 years are destroyed; new documents will be destroyed after 3 months. The paper evidence should be kept available in alignment with Circular 319 (Rule 6), which stipulates that records must be kept "until the reimbursement is made".

Purpose of Processing Records of different nature and scope are archived for administrative, institutional, legal and historical purpose, as applicable. Most importantly, in view of the clear role of the Council Secretariat in preserving institutional memory of the EPO, the Council Secretariat has kept the records of CA documents and other business-relevant paper or electronic files since end of the 1970s .

Data subjects and categories of personal data

Externals

Contact Information	
Contact Details	Country
Home Address	Mobile Phone Number

Phone Numbers	Working email address
Correspondence	
Personal information provided voluntarily	
Employment Information	
Company Entity	Department name and/or number
Job Title Role	Language preference (of communication)
Office Location	
Personal Identification	
First Name	Full Name
Gender	Nationality
Picture	

Former Employees

Contact Information	
Contact Details	Country
Home Address	Mobile Phone Number
Personal Email	Phone Numbers
Employment Information	
Department name and/or number	Duration of employment
End Date	Job Title Role
Start Date	
Personal Identification	
First Name	Full Name
Gender	Surname
Nationality	Picture

Prospective Employees

Contact Information	
Contact Details	Country

Home Address	Personal Email
Phone Numbers	
Correspondence	
Personal information provided voluntarily	
Personal Identification	
First Name	Full Name
Gender	Surname
Nationality	

Recipient of the personal data

Recipients of the data Recipients within the EPO include individuals from different operational units upon request and upon assessment of their business case.

1. recipients within the European Patent Office:
a) Paper copies and scanned CA and CA/C documents already uploaded and available on the dedicated MICADO Documents and MICADO-C databases: all Office employees have access to the MICADO Documents. MICADO-C has a defined list of internal users
b) Other records not stored in the MICADO Documents repositories: Directorate General DG 5 Legal Services, President's Office, upon request following approval by the Head of the Council Secretariat after assessment of the business case may have access to certain parts of the information on a need-to-know basis. (e.g. information on litigation cases for the preparation of legal defence)
c) Specialised services: administrative documents (travel sheets and reimbursement to delegates and experts): they are temporarily kept for accounting and auditing purposes and the scanned copies are sent to the Pension and specialised services, as applicable, for further processing.

2. recipients within the European Patent Organisation or national offices of Member States: upon request following approval by the Head of the Council Secretariat after assessment of the business case may have access to certain parts of the information on a need-to-know basis (e.g. for historical purposes regarding documents not available electronically on MICADO before 1996).
3. External processors

4. Third parties request by the general public (for example for academic research): after assessment of the business case and in consultation with Legal Services the Council Secretariat may give access to documents stored on a need-to-know basis. The personal data would - whenever possible - be anonymised.

Purpose of sharing

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors) SAP - Germany, Microsoft - United States, OpenText - United Kingdom

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 406

Name EPO Together

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 45 - CTO / BIT

Entity Name - Controller (Entities) DG0 - 02 - Communication

External processors

Spatial Chat

External processors	
Name Spatial Chat	

Description of the processing

Description Personal data collected by the data controller is provided directly from the data subject when they join any meetings held through the EPOtogether tool, which is a cloud-based platform developed by the external provider “Spatial Chat”. The tool is accessed through the data subject’s web browser and thus does not need to be installed on their computer.

To join the platform, only the necessary identification data is requested (they will be asked to give their email address only the first time they join the platform or until they delete the related cookies on their web browser).

Additionally, data subjects are free to include more information, such as their name and surnames, personal information about them, as well as a picture (personal or not).

As the tool’s core features include business messaging, calling, audio and video meetings and file sharing, additional personal data may be collected in the course of a meeting, event, presentation, as well as one-on one conversation. Consequently, participants to a meeting/event on a social room will also be able to see users’ email address (and therefore potentially their name and surnames) in case of any questions/comments.

Recordings (audio-visual personal data) and live captions taken by the data controller during a meeting/event are stored in the data controller’s database, to whom only authorised people with the status of "administrator" have access. The audio-visual material might be edited and published on the EPO internal (e.g., Intranet, EPO TV) and external platforms (e.g., EPO website, e-knowledge Portal), for information and promotional purposes, and thus your personal data such as image and voice. Once the recording has been edited, data controller will only keep the minimum and necessary personal data in their database to fulfil the
promotional purpose. Personal data disclosed to the public through the EPO internal and external channels will be deleted according to the audio-visual retention policy of the EPO.
Regarding the interactions of the users on the social rooms, any content that they have shared on the board will disappear after they leave the room. On the contrary, information, statements and material shared on the chat remain until the organiser of the meeting/event deletes the space.

In the same line with the above, the organiser of an event shall delete the space or room created after the event, to avoid that people who have visited an event have access to future events unless invited.

Personal data are also collected by the data controller through the tool for analytical purposes (e.g., statistics).

Additionally, personal data may be processed for maintaining the performance of the Spatial Chat Services, complying with legal obligations, and resolving disputes. Spacial Chat may retain logs of automatically collected information (for internal statistics and security purposes).

Purpose of Processing Manage discussions, presentations, questions and answers organised in the social and stage rooms, Giving access to participants to join any specific rooms, Recording or taking live captions of any event taking place in the Stage room for editing and subsequent publication on the EPO internal (e.g., Intranet, EPO TV) and external platforms (e.g., EPO website, e-knowledge Portal), Organising meetings and events, Coordinating any technical issues affecting the execution of the event that may arise before, during or after the event takes place, Sharing information, videos, links, interactions (gifs and emojis), Analytical purposes (e.g., statistics), Providing to EPO employees a platform where they can interact and socialise in a virtual space, Providing end-user support and troubleshooting for the platform and features

Data Retention Personal data processed by the data controller or the service providers under its supervision are generally stored for the period of time necessary to achieve the purpose for which they have been processed.

Information necessary to join the platform and voluntary information and personal picture uploaded to the users' profile will be retained until they clear cookies from their device. Nevertheless, contact details such as email address, name and surname can be kept for a longer period by the controller and in accordance with the general data protection statement for meetings and events.

For the personal data shared on the spaceboard, they are stored until the user who shared the information or material (e.g., video, gif, presentation) leaves the space/room.
For the personal data shared in the tool, they are stored until the space/room is deleted by the administrator and for a maximum period of 6 months.

Personal data contained in the recordings are stored and deleted according to the general data protection statement for meetings and event, and the EPO audio-visual retention policy.
Additionally, personal data may be processed for maintaining the performance of the Spatial Chat Services, complying with legal obligations, and resolving disputes. Spacial Chat may retain logs of automatically collected information (for internal statistics and security purposes).

In the event of a formal appeal/litigation, all data held at the time the formal appeal/litigation was initiated will be retained until the proceedings have been closed.

Data subjects and categories of personal data

Employees

Online invigilation data	
Audio input	Webcam captures
Employment Information	
Company Entity	Contract Type
Office Location	
Personal Identification	
First Name	Full Name
Gender	Surname
Picture	
Geolocation	
Geolocation Information	
Matter/Log file	
Attachments	Metadata

General	
Any other information	
Network/application Interaction Data	
Session content	Session details
Session metadata	
Contact Information	
Working email address	
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Learning external events
Professional Experience & Affiliations	
CV	
Device Management Data	
Account ID	Last Logon Time
Managed Application Installation Location	
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Browsing Information	
Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
Category	Cookie Information
IP Address	Network Interaction History
URL	Website History
User Account Information	
User ID	
System Logs	
File data (name, size and/or hash)	System-, Application-, Security-related Server Logs
Web Servers Logs	

Externals

Sensory and Electronic Information	
Audio Information	Visual Information
Telephony Interaction Data	
Recorded Audio File	
Online invigilation data	
Audio input	Webcam captures
Employment Information	
Language preference (of communication)	
Personal Identification	
First Name	Full Name
Gender	Picture
Matter/Log file	
Attachments	Metadata
General	
Answers to surveys, assessments or quizzes	Any other information
Network/application Interaction Data	
Session content	Session details
Session metadata	
Contact Information	
Contact Details	Working email address
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	
Professional Experience & Affiliations	
CV	
Device Management Data	
Account ID	Last Logon Time
Managed Application Device Tag	
Correspondence	

Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Browsing Information	
Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
Category	Cookie Information
IP Address	Network Interaction History
URL	Website History
User Account Information	
User ID	
System Logs	
File data (name, size and/or hash)	System-, Application-, Security-related Server Logs
Web Servers Logs	

Recipient of the personal data

Recipients of the data - EPO staff working in PD Communication and BIT on a need-to-know basis
- EPO employees with an Administrator status
- Third-party service providers for maintenance and support purposes
- Users of the EPOtogether tool (only for the personal data shared with them when participating to an event/meeting)
- General public (only for the personal data shared with them when participating to an event/meeting).

Purpose of sharing - User authentication and access control for the purposes of managing the meetings and events hosted on the tool
- Maintenance and support purposes provided by the EPO staff with an administrator status as well as the external provider Spatial Chat
- Voluntary information provided by the data subject as well as named comments and questions are shared with the users of the tool for transparency purposes
- Recordings and live captions might be shared with the EPO staff or the general public through the EPO internal and external channels for promotional purposes

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 417

Name Constitution of the Jury Members' Panel for the European Inventor Award and Young Inventors prize

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG1 - 11 - COO

Entity Name - Controller (Entities) DG0 - 02 - Communication

External processors

Award Force Pty Ltd

External processors	
Name Award Force Pty Ltd	

Creative Force Ltd

External processors	
Name Creative Force Ltd	

Description of the processing

Description Every year, the jury is composed of former finalists of the European Inventor Award & Young Inventors Prize. In order to facilitate communication and collaboration with them, in 2023 the European Inventor Network was created. This is a network that allow the EIA team to manage the contact details of the finalists. Thus, by using the information provided by this list, finalists previously selected by the EIA team are contacted and offered the possibility of being part of the jury in an edition.

In the event they accept, the necessary personal data, such as email address and their availability, are processed by the EIA team, so that they receive all the
information about the nominees and vote. This also allow the controller to collect the professional feedback from the jury members by email exchange and
through Awardforce in order to select the finalists of the edition.

In addition, to promote their participation on the EPO's internal (e.g.: Intranet) and external communication platforms (e.g.: EPO website, EPO social media
platforms, European Inventor Award Newsletter and the external contractor event platform), they are informed that personal data such as personal photos of
them and statements about the finalists may be collected.

The personal data associated with the organisation of the Jury meeting or collected during the voting process which is not needed afterwards are manually
erased latest after 6 months following the last action in relation to the event.
Personal data such as contact details that the controller has included on the list of the European Inventor Network are manually updated during the course of
the voting process.

Purpose of Processing Carrying out the jury deliberation meeting, Managing and updating the European Inventor Network, Promoting their participation on the EPO's internal and external channels, Allowing jury members to vote through the online platform

Data Retention Personal data processed by the data controller or the service providers under its supervision are generally stored for the period of time necessary to achieve the purpose for which they have been processed.

The personal data associated with the organisation of the Jury meeting must be erased latest after 6 months following the last action in relation to the event.

Nevertheless, some personal data might be kept for a longer period of time as follows:

For personal data related to sound, video and audio-visual recording/photographs of meetings and events, they are stored for educational, institutional, historical, informational and/or promotional purposes for a period ranging from 2, 10 or 25 years according to the retention categories reflected in the PD Communication Audio-visual Retention Policy, which can be provided upon request. Events that can fall in the aforementioned retention categories are:
o Recurrent events with a low level of newsworthiness (2 years renewable);
o Non-recurrent events related to the core business of the EPO, for example related to the
promotion of patent knowledge activities (10 years renewable);
o Recurrent events with a high level of newsworthiness related to the core activity of PD
Communication at the EPO (e.g.: European Inventor Award, European Patent Convention 50
years celebration) (25 years renewable).

Such data may be published on the EPO intranet, the EPO website, or made available via the Office's other social media channels or the e-knowledge Portal. If this is the case, personal data will be limited as much as possible, for example, by keeping only the name, surname, and photographs.

For personal data related to contact details (e.g.: name, surname, email address, affiliation) they are stored for and deleted after a maximum period of 5 years as part of an internal EPO contact details database owned by PD Communication and shared internally among EPO organisational units in order for them to contact data subjects for similar future meetings/events.

At any moment the data subject may exercise his or her rights and ask for being removed from the list. This request does not affect the lawfulness of the
processing prior to the exercising of his or her rights.

Regarding the content published on EPO's internal and external channels due to the data subject's participation as jury member in the European Inventor Award or any other conference/meeting/event, the content will remain and be processed according to the respective privacy policies.

In the event of a formal appeal/litigation, all data held at the time of the formal appeal/litigation shall be retained until the completion of its process.

Data subjects and categories of personal data

Externals

Sensory and Electronic Information	
Audio Information	Visual Information

Contact Information	
Contact Details	Country
Mobile Phone Number	Personal Email
Working email address	
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	
Professional Experience & Affiliations	
CV	
Correspondence	
Additional Information which might be provided in the course of exchanges	Personal information provided voluntarily
Employment Information	
Job Title Role	Language preference (of communication)
Personal Identification	
First Name	Full Name
Surname	

Recipient of the personal data

Recipients of the data The personal data might be disclosed to:
- The EPO staff working in Principal Directorate Communication (PD Communication)
- Other EPO organisational units
- The external contractors involved in the organisation of the event on a need-to-know-basis.
- Third-party external providers.
- EPO employees with access to the Intranet.
- Multipliers
- General public accessing the EPO website, or any other external communication channel used by Principal Directorate Communication (PD Communication).

Purpose of sharing To allow the correct organisation of the constitution of the jury members as well as the voting process and meetings.
- For maintenance purposes.
- To highlight and promote the importance of the role played by the jury members in the European Inventor Award & Young Inventors Prize event.
- To facilitate communication and future collaborations with the jury members of each edition.

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 418

Name User Experience (UX) research on EPO software applications

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 46 - CIO / BIT

Entity Name - Controller (Entities) DG4 - 45 - CTO / BIT

External processors

Figma

External processors	
Name Figma	

Lighting Beetle

External processors	
Name Lighting Beetle	

Figma

External processors	
Name Figma	

Microsoft

External processors	
Name Microsoft	

ServiceNow

External processors	
Name ServiceNow	

Description of the processing

Description UX design, or User experience design, is a multidisciplinary field focused on creating user-centric products, services, and systems. Starting from ergonomics, UX design encompasses the entire user journey when interacting with a product or service.
At the Office, UX design ensures the EPO's tools are not only functional but also user-friendly, making navigation seamless and tasks efficient for patent examiners and legal professionals.
The EPO's UX philosophy hinges on user-centricity, accessibility, and continuous improvement. BIT 4514 User Experience department strives to understand end-users' unique challenges, translating this understanding into intuitive application interfaces and streamlined processes. At the Office, UX design is a collaborative journey that involves everyone, including first and foremost the end users.
The best insights come from those who use the EPO's systems daily; their valuable feedback and active participation play a vital role in shaping the EPO's UX enhancements.
BIT User Experience team collects and processes quantitative and qualitative data from application end-users. The purpose is to get statistically solid, representative figures about user satisfaction with EPO products and services.
For this purpose, the UX team applies various methods and tools such as:
• generative research methods with the purpose of identifying user needs especially but not exclusively: user interviews, surveys, diary studies, and any other method usually used for the purpose of identifying user needs; any method for achieving that purpose can be conducted either in person or via digital means;
• evaluative research methods with the purpose of validating design solutions and ideas especially but not exclusively: usability testing, prototype testing, A/B testing, and any other method usually used for the purpose of validating design solutions and ideas; any method can be conducted either in person or via digital means;
• analysis of user feedback and data extracted from analytics tools especially, but not exclusively: from Matomo (see https://matomo.org/features/), from customer support platforms (e.g. Service Now), or other user channels, (e.g. MS-Teams chats), and from any other tool usually used for the purpose of collecting user feedback and data.

By means of all the above, UX design empowers EPO applications' end-users, enhances productivity, and supports the European Patent Office's mission.

Data Retention The retention time of personal data processed in the current processing operation is three months. By the end of the retention period, anonymised reports are created and the source original personal data are deleted for good.

Purpose of Processing The purpose of the processing operation is to collect feedback from internal and external users of IT tools developed and/or deployed at the EPO in order to identify their requirements, preferences, pain points and suggestions for improvements. The ultimate goal is to enhance their user experience.

Data subjects and categories of personal data

Employees

General	
Answers to surveys, assessments or quizzes	Any other information

Ticketing	
Ticket related data	
Physical and/or Digital Identifiable Assets	
Operating System Version	
Sensory and Electronic Information	
Audio Information	Visual Information
Contact Information	
Working email address	
Building area and site	
Building area and site	
Representation in EPO's Patent Granting Process	
Role in the Patent Grant Procedure	
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Employment Information	
Department name and/or number	Duration of employment
Job Title Role	Language preference (of communication)
Line Reporting Manager	Office Location
Browsing Information	
Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
Category	Cookie Information
IP Address	Network Interaction History
Search query	URL
Website History	
Personal Identification	

Disability or Specific Condition	
Geolocation	
Geolocation Information	
User Account Information	
Application Specific User Role	

Externals

General	
Answers to surveys, assessments or quizzes	Any other information
Ticketing	
Ticket related data	
Physical and/or Digital Identifiable Assets	
Operating System Version	
Sensory and Electronic Information	
Audio Information	Visual Information
Contact Information	
Working email address	
Representation in EPO's Patent Granting Process	
Role in the Patent Grant Procedure	
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Employment Information	
Department name and/or number	Job Title Role
Language preference (of communication)	
Browsing Information	
Browser User Agent	Browsing Date and Time
Browsing Time	Category
Cookie Information	IP Address

Network Interaction History	Search query
URL	Website History
Personal Identification	
Disability or Specific Condition	First Name
Full Name	Surname
Geolocation	
Geolocation	
User Account Information	
Application Specific User Role	

Recipient of the personal data

Recipients of the data Recipients of the personal data are the 4514 User Experience team staff members and the Director of 4.5.1 Enterprise Architecture.

Purpose of sharing Personal data are shared to 4514 UX staff members to create consolidated reports on the collected data. The consolidated reports will contain no personal data; they will feature only aggregated data and the corresponding analysis.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors) ServiceNow - Netherlands, Figma - United States, Microsoft - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures	Specific members of UX team are granted permission to record interviews/testing sessions with EPO users, according to their specific role, assignment and need-to-know; such permissions are checked and revalidated/removed on annual basis., EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 420

Name EPO Art collection management

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 46 - CIO / BIT

Entity Name - Controller (Entities) DG4 - 4 - Corporate Services

External processors

zetcom

External processors	
Name zetcom	

Description of the processing

Description The EPO manages an art collection composed of valuable objects (pieces of art) and their associated features throughout their lifecycle.

For this, the EPO uses a collection management software which allows for comprehensive cataloguing, registration, and management of all objects in the collection, as well as the management of digital media linked to objects, artists, addresses, and other entries. Additionally, the software facilitates the management of agreements and contracts relating to exhibitions, loans, and collection objects, as well as the coordination of participants, venues, and lenders. The software also provides additional modules such as event management and archiving, which can be seamlessly integrated into the software.

Data Retention Data are kept for 50 years aftre the piece of art has left the collection

Purpose of Processing Management of the EPO art collection

Data subjects and categories of personal data

Externals

Browsing Information

IP Address	
Personal Identification	
First Name	Full Name
User Account Information	
Account Password	Ownership Permissions
User ID	

Employees

Physical and/or Digital Identifiable Assets	
Installed Software Applications	
Browsing Information	
IP Address	
Personal Identification	
First Name	Full Name
User Account Information	
Ownership Permissions	Password
User ID	

Recipient of the personal data

Recipients of the data EPO art collection manager in the President Office
EPO staff of the EPO art team

Purpose of sharing

Transfer

Transfer No

Country where data might be transferred - Processor (Vendors)

Transfer to public authority and/or International Organisation

Reasons for the transfer

Transfer mechanism(s)

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 426

Name Management of the MICADO Address Book (MAB) - SC

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG5 - 501 - Council Secretariat

External processors

Zoom

External processors	
Name Zoom	

OpenText

External processors	
Name OpenText	

Microsoft

External processors	
Name Microsoft	

Zoom

External processors	
Name Zoom	

Microsoft

External processors	
Name Microsoft	

Linkando

External processors	
Name Linkando	

Description of the processing

Description MICADO Address Book (MAB): The CS collects, records, stores and updates personal data of selected EPO employees, delegates of member and observer states, non- governmental organisations, intergovernmental organisations, and external consultants participating in Select Committee meetings in a dedicated database called MICADO Address Book (MAB).
MAB is accessible in MICADO which is a database managed by the Council Secretariat (CS). To access the MICADO database, user accounts are created for external users and need to be approved by the CS. MICADO users have access (read-only) to the MAB. EPO employees need to request MAB access to CS separately.
CS performs mainly the following actions:
(1) Collection: Personal data are usually provided by the data subject, notably members of the Select Committee, when announcing their participation to a meeting. The remainder is provided upon request by CS. MAB includes single records that can be printed, extracted and sorted in a preferred way and are constantly updated.
(2) Deactivation: Due to the changes in a delegation's composition (e.g. retirement, delegate no longer forming part of their delegation), the CS deactivates the access rights to MAB (see following paragraph) and set the record as non-public. In this case, these records are only accessible by the CS. The accounts of the EPO employees are deactivated automatically at the end of their service and hence will not be able to access MAB.

Data Retention A. Authorised MICADO Documents users (notably this group includes delegates): They are deleted upon request by the data subject. Otherwise they are marked as non-public and therefore are not visible to other users, but they remain accessible to the CS as long as such data can be needed e.g. in the process of finding suitable candidates for certain Committees' positions. EPO employees' data are deleted in MAB after they leave the Office. If a former EPO employee becomes a member in the Select Committee after retirement (a rare occurrence) a new record will be created then.
B- External experts and consultants: personal data are kept as long as obligations by the Office exist including adequate time to check the fulfilment of those obligations.
C- Members of the Board of auditors and its experts: personal data are kept as long as obligations by the Office exist, including adequate time to check the fulfilment of those obligations.

Purpose of Processing Personal data are processed to ensure the organisation, administration and running of the SC business; to keep historical record on composition of the SC; to fulfil contractual obligations of the European Patent Organisation towards Council expert.

Data subjects and categories of personal data

Employees

Contact Information

Contact Details	Country
MICADO ID user number	Mobile Phone Number
Phone Numbers	Working email address
Correspondence	
Personal information provided voluntarily	
Employment Information	
Department name and/or number	Duration of employment
End Date	Job Title Role
Language preference (of communication)	Office Location
Start Date	
Personal Identification	
First Name	Gender
Surname	Nationality
Picture	

Externals

Contact Information	
Contact Details	Country
MICADO ID user number	Mobile Phone Number
Phone Numbers	Working email address
Correspondence	
Personal information provided voluntarily	
Employment Information	
Department name and/or number	Duration of employment
End Date	Job Title Role
Language preference (of communication)	Office Location
Personal Identification	
First Name	Full Name

Gender	Surname
Nationality	Picture

Recipient of the personal data

Recipients of the data The members of the Select Committee having MICADO Documents access have access to personal data which are defined as public: Member state, preferred language, last name, first name, postal address of the employer, email address and phone numbers. Participation and a role of a member in the Council's bodies is also visible as far as defined in MAB.

All other private information as well as records of the EPO employees and inactive records can be seen only by MAB administrators (i.e. D501 staff having full access rights to MAB and being able to add, change and delete records).

Personal data depending on its type and the purpose of its processing is made accessible on a need-to-know basis to Heads of delegation and their alternates (Council), Board of Auditors, and the external providers/their sub-contractors.

Directorate General DG 5, President's Office, upon request following approval by the Head of the Council Secretariat after assessment of the business case may have access to certain public parts of the information stored on the contact details database on a need-to-know basis.

External processors

Data published online (MICADO-P and EPO website) will be accessible by the general public.

Purpose of sharing See 1.16

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards, Data Protection EU Comm Standard Contractual Clauses

Country where data might be transferred - Processor (Vendors) Microsoft - United States, Zoom - United States, OpenText - United Kingdom

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 433

Name Archiving of Select Committee's documents which include personal data

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG5 - 501 - Council Secretariat

External processors

SAP

External processors	
Name SAP	

OpenText

External processors	
Name OpenText	

Microsoft

External processors	
Name Microsoft	

Description of the processing

Description SC documents are uploaded and made available on the dedicated MICADO-U and MICADO-UC databases. These are repositories for the SC documents managed by Council Secretariat, while MICADO-UC contains only the SC confidential documents.

Purpose of Processing Records of different nature and scope are archived for administrative, institutional, legal and historical purpose, as applicable.

Data Retention SC and SC/C documents made available on MICADO-U and MICADO-UC respectively are kept indefinitely

Data subjects and categories of personal data

Externals

Contact Information	
Contact Details	Country
Home Address	Mobile Phone Number
Phone Numbers	Working email address
Correspondence	
Personal information provided voluntarily	
Employment Information	
Company Entity	Department name and/or number
Job Title Role	Language preference (of communication)
Office Location	
Personal Identification	
First Name	Full Name
Gender	Nationality
Picture	

Former Employees

Contact Information	
Contact Details	Country
Home Address	Mobile Phone Number
Personal Email	Phone Numbers
Employment Information	
Department name and/or number	Duration of employment
End Date	Job Title Role
Start Date	
Personal Identification	

First Name	Full Name
Gender	Surname
Nationality	Picture

Prospective Employees

Contact Information	
Contact Details	Country
Home Address	Personal Email
Phone Numbers	
Correspondence	
Personal information provided voluntarily	
Personal Identification	
First Name	Full Name
Gender	Surname
Nationality	

Recipient of the personal data

Recipients of the data Users with access to MICADO-U and MICADO-UC respectively are:.

1. recipients within the European Patent Office: SC and SC/C documents made available on MICADO-U and MICADO-UC respectively are kept indefinitely: all Office employees have access to the MICADO-U Documents. MICADO-UC has a defined list of internal users.

2. External processors.

3. Third parties request by the general public (for example for academic research): after assessment of the business case and in consultation with Legal Services the Council Secretariat may give access to documents stored on a need-to-know basis. The personal data would - whenever possible - be anonymised.

Purpose of sharing

Transfer

Transfer No

Country where data might be transferred - Processor (Vendors) SAP - Germany, OpenText - United Kingdom, Microsoft - United States

Transfer to public authority and/or International Organisation

Reasons for the transfer

Transfer mechanism(s)

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 434

Name Contractor management (creation, on/offboarding, deletion of EPO external contractors)

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 44 - General Administration

Entity Name - Controller (Entities) DG4 - 46 - CIO / BIT

External processors

SAP

External processors	
Name SAP	

ServiceNow Inc. (USA)

External processors	
Name ServiceNow Inc. (USA)	

Microsoft

External processors	
Name Microsoft	

ServiceNow

External processors

Name	
ServiceNow	

Description of the processing

Description The EPO's external contractors lifecycle is managed through the Contractor Management processing operation. Contractor Management applies to contractors working in any EPO organisational unit.
The processing operation is based on the integration of business logic and data referred to the given contract, the vendor, the contract's team members, the contract administrators, the contractors.
Through a ServiceNow front-end application, EPO contract managers can directly create, associate, de-associate, delete contractor entries referred to a contract, as well as extend them and provide them with needed equipment and resources (e.g. badge, software licenses, VDI, etc). EPO contract managers will only be able to extend or on-/off-board contractors of contracts they are responsible for; they may also use delegation, either by : a) delegating another EPO staff member to act as EPO contract manager on their behalf ; or b) delegating an external contract manager (such a thing demands prior approval step by the EPO contract manager or by his/her delegate(s).

Data Retention The EPO's Contractor Management processing operation has been in place since January 2024 and processes personal data of EPO contractors who have been onboarded from such date onwards.
A contractor' s personal data and the information about the associated contract and vendor are stored within the (ServiceNow-based) "Contractor Management" application to pursue the stated purposes, in compliance with the EPO's Data Protection Rules, EPO's Retention Policy and EPO's Retention Schedule.
Currently the tasks within EPO's "Contractor Management" processing operation are subject to the same default retention period (5 years) as the tasks in the "Workflow, Data and Knowledge Management based on EPO ServiceNow capabilities" processing operation.
Within the “Contractor Management” application, data of contractors who get removed from a contract are not deleted, but updated by appending the removal date; this is justified by efficiency reasons and by the need to facilitate re-hires and extensions.

Purpose of Processing Personal data are processing for the following purposes: 1. to facilitate the creation, on- and off-boarding, deletion of EPO contractors in the EPO's master source systems by means of a front-end application integrated into ServiceNow; 2. to manage the allocation of each contractor to the corresponding contract and manage related processes; 3. to make available an audit trails of each operation performed.

Data subjects and categories of personal data

Contractors

Physical and/or Digital Identifiable Assets	
IMEI Number (International Mobile Equipment Identity)	Mobile Device Name
Mobile Device Serial Number	Vendor Model of Workstation
Workstation Serial Number	Workstation's Hostname (Physical or Virtual)
Contact Information	
Working email address	
Building area and site	
Building area and site	

Device Management Data	
Account ID	AppleID for iOS/iPadOS Devices
Azure Active Directory Device ID	EAS Device ID
Encryption Keys	Intune Device ID
Intune Device Management ID	Last Logon Time
MAC Address	Managed Application Device Tag
Managed Application ID	Managed Application Installation Location
Managed Application Name	Managed Application Size
Managed Application Version	Platform-specific IDs
Tenant ID	Windows ID for Windows Devices
Employment Information	
Company Entity	Contract Type
Department name and/or number	End Date
Language preference (of communication)	Line Reporting Manager
Office Location	Personnel Number
Start Date	Working patterns
Personal Identification	
Date of Birth	First Name
Gender	Surname
Nationality	Signature
User Account Information	
Application Specific User Role	Third-party User Identifier
User ID	

Employees

Contact Information	
Working email address	

Personal Identification	
First Name	Surname
User Account Information	
Application Specific User Role	User ID

Externals

Contact Information	
Working email address	
Employment Information	
Company Entity	Contract Type
Department name and/or number	Language preference (of communication)
Office Location	Working patterns
Personal Identification	
Date of Birth	First Name
Gender	Surname
Nationality	Signature

Recipient of the personal data

Recipients of the data Possible recipients of personal data are:
- ServiceNow users who are assigned any of these roles: EPO contract administrator, vendor administrator, additional EPO contract administrators, additional vendor administrators. Depending on their profile as defined in iValua PaSP (Procurement and Sourcing Portal) with regard to the given contract, in ServiceNow Contractor Management they are either added as the main EPO/vendor administrator, or one of the additional ones.

- Centralised team of administrators who receive an (approved) onboarding task in ServiceNow with all of the required information and enter a new user in SAP.

- SAP. Further to onboarding, contract administrators may perform other actions from within the Contractor Management application. Such updates include extensions, re-hire, (premature) offboarding etc. These will generate requests accordingly, which equally require an EPO approval if initiated by one of the vendor contractor administrators. Unlike in case of onboarding requests, none of the resulting updates require the involvement of the central administrator team.

Purpose of sharing Personal data are shared to users having either the role "EPO contract administrator", or the role "vendor administrator" , or the role "additional EPO contract administrator", or the role "additional vendor administrator" for the purpose of administering the given contract.

Personal data are shared to the centralised team of administrators in order for said administrators:
to onboard new contractors into SAP;
to request a re-hire of a contractor, in case such person already existed within SAP;
for exception handling purposes.

Transfer

Transfer Yes

Country where data might be transferred - Processor (Vendors)
Microsoft - United States, SAP - Germany, ServiceNow - Netherlands

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards, Data Protection EU Comm Standard Contractual Clauses

Reasons for the transfer Customer support and incident resolution (e.g. security) purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums)., ServiceNow PHYSICAL SECURITY MEASURES: -DATA CENTER FACILITIES. ServiceNow data centre facilities include (1) physical access restrictions and monitoring that shall include a combination of any of the following: multi-zone security, man-traps, appropriate perimeter deterrents, on-site guards, biometric controls, CCTV and secure cages; (2) fire detection and fire suppression systems both localised and throughout the data center floor. -SYSTEMS, MACHINES AND DEVICES. The systems, machines and devices include (1) physical protection mechanisms; and (2) entry controls to limit physical access. -MEDIA. ServiceNow shall use NIST 800-88 industry standard (or substantially equivalent) destruction of sensitive materials, including Customer Data, before such media leaves ServiceNow's data centers for disposition. ServiceNow TECHNICAL SECURITY MEASURES: -ACCESS ADMINISTRATION. Access to the EPO's ServiceNow by ServiceNow employees and contractors is protected by authentication and authorization mechanisms. User authentication is required to gain access to production and sub-production instances. Individuals are assigned a unique user account. Individual user accounts shall not be shared. Access privileges are based on job requirements using the principle of least privilege access and are revoked upon termination of employment or consulting relationships. Access entitlements are reviewed by management quarterly. Infrastructure access includes appropriate user account and authentication controls, which will include the required use of VPN connections, complex passwords with expiration dates, account lock-out enabled, and a two-factor authenticated connection. -SERVICE ACCESS CONTROL. The ServiceNow service provides user and role-based access controls. The EPO is responsible for configuring such access controls within its instance. -LOGGING AND MONITORING. The production infrastructure log activities are centrally collected, are secured in an effort to prevent tampering, and are monitored for anomalies by a trained security team. ServiceNow shall provide a

logging capability in the platform that captures login and actions taken by users in the ServiceNow application. The EPO has full access to application audit logs within own ServiceNow instances, including successful and failed access attempts. The EPO is responsible for exporting application audit logs to Customer's syslog server through available built-in platform features. -FIREWALL SYSTEM. An industry-standard firewall is installed and managed to protect ServiceNow systems by residing on the network to inspect all ingress connections routed to the ServiceNow environment. ServiceNow managed firewall rules are reviewed quarterly. The EPO shall be responsible for reviewing any Customer managed firewall rules on its instances. -VULNERABILITY MANAGEMENT. ServiceNow conducts quarterly security risk evaluations to identify critical information assets, assess threats to such assets, determine potential vulnerabilities, and provide for remediation. When software vulnerabilities are revealed and addressed by a vendor patch, ServiceNow will obtain the patch from the applicable vendor and apply it within an appropriate timeframe in accordance with ServiceNow's then-current vulnerability management and security patch management standard operating procedure and only after such patch is tested and determined to be safe for installation in all production systems. -ANTIVIRUS. ServiceNow updates antivirus, anti-malware, and anti-spyware software on regular intervals and centrally logs events for effectiveness of such software. -CHANGE CONTROL. ServiceNow evaluates changes to platform, applications, and production infrastructure to minimize risk and such changes are implemented following ServiceNow's standard operating procedure. -DATA SEPARATION. Customer Data shall be maintained within a logical single-tenant architecture on multi-tenant cloud infrastructure that is logically and physically separate from ServiceNow's corporate infrastructure. -CONFIGURATION MANAGEMENT. ServiceNow shall implement and maintain standard hardened configurations for all system components within the service subscribed by the EPO. ServiceNow shall use industry standard hardening guides, such as guides from the Center for Internet Security, when developing standard hardening configurations. -DATA ENCRYPTION IN TRANSIT. ServiceNow shall use industry standard encryption to encrypt EPO's data in transit over public networks to the ServiceNow Service. -DATA ENCRYPTION AT REST. ServiceNow shall provide encryption at rest capability for column level encryption, which the EPO may enable at its sole discretion. -SECURE SOFTWARE DEVELOPMENT. ServiceNow shall implement and maintain secure application development policies and procedures aligned with industry standard practices such as the OWASP Top Ten (or a substantially equivalent standard). All personnel responsible for secure application design and development will receive appropriate training regarding ServiceNow's secure application development practices. -SECURE CODE REVIEW. ServiceNow shall perform a combination of static and dynamic testing of code prior to the release of such code to Customers. Vulnerabilities shall be addressed in accordance with its then current software vulnerability management program. Software patches are regularly made available to Customers to address known vulnerabilities. -ILLICIT CODE. The ServiceNow service shall not contain viruses, malware, worms, date bombs, time bombs, shut-down devices, that may result in, either: (a) any inoperability of the service; or (b) any interruption, interference with the operation of the service. If the service is found to contain any illicit Code that adversely affects the performance of the service or causes a material security risk to EPO's Data, ServiceNow shall, as EPO's exclusive remedy, use commercially reasonable efforts to remove the illicit Code or to advise and assist EPO to remove such illicit Code. ServiceNow ORGANISATIONAL SECURITY MEASURES: -DATA CENTER INSPECTIONS. ServiceNow performs routine reviews of data centers to confirm that the data centers continue to maintain appropriate security controls necessary to comply with its own Security Program. -PERSONNEL SECURITY. ServiceNow performs background screening on all employees and all contractors who have access to EPO's Data in accordance with ServiceNow's then-current applicable standard operating procedure and subject to Law. -SECURITY

AWARENESS AND TRAINING. ServiceNow maintains a security and privacy awareness program that includes appropriate training and education of ServiceNow personnel, including any contractors or third parties that may access EPO's Data. Such training is conducted at time of hire and at least annually throughout employment at ServiceNow. -VENDOR RISK MANAGEMENT. ServiceNow maintains a vendor risk management program that assesses all vendors that access, store, process, or transmit EPO's Data for appropriate security and privacy controls and business disciplines. -SOFTWARE AND ASSET INVENTORY. ServiceNow shall maintain an inventory of all software components (including, but not limited to, open source software) used in EPO's ServiceNow service, and inventory all media and equipment where EPO Data are stored. -WORKSTATION SECURITY. ServiceNow shall implement and maintain security mechanisms on personnel workstations, including firewalls, anti-virus, and full disk encryption. ServiceNow shall restrict personnel from disabling security mechanisms. ServiceNow's committments abour own CERTIFICATIONS AND ATTESTATIONS: ServiceNow shall establish and maintain sufficient controls to meet certification and attestation for the objectives stated in ISO 27001, ISO 27018, SSAE 18 / SOC 1 and SOC 2 Type 2 (or equivalent standards) for the Security Program supporting the Subscription Service. At least once per calendar year, ServiceNow shall obtain an assessment against such standards and audit methodologies by an independent third-party auditor and make the executive reports available to the Customer. In the Contract Management application, any addition or removal of deputy contract administrators is kept aligned - via regularly scheduled jobs - with the master information on the contract's team composition, defined in iValua.

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 435

Name Formal complaint and feedback

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 46 - CIO / BIT, DG1 - 13 - Quality and Practice Harmonisation

Entity Name - Controller (Entities) DG1 - 15 - Customer Journey and KAM

Description of the processing

Description Users of the Patent system can submit complaints or feedback using an electronic form which is available at the EPO website via the Formal complaint / feedback form link in the "Contact us" page of the EPO website. Complaints or feedback may also be submitted via a telephone call to the First Line Customer Enquiries Unit (1LCEU) or by sending a letter addressed to the EPO, to the President, to a Vice-President or to a Director.

A case is always created and registered in a database, currently ServiceNow, a registration number in the form "CS123456" is generated, and the case is assigned to the "External Complaints" group of PD15 and PD13 for further processing. Once a case is registered as a complaint or feedback, an automated acknowledgement of receipt is sent to the user by email.

Processing of the complaint or feedback includes the steps of analysing the user's input, contacting the department dealing with the corresponding service, dialogue with regard to the root cause of the possible issue, and compiling a reply to the user within 20 days of the date of submission of the complaint or feedback.

External complaints/feedback can concern any service or product delivered by the EPO and can be submitted by any person, including parties to proceedings before the EPO (for enquiries as to the processing of files, see Guidelines for Examination in the European Patent Office E VIII, 7). Complaints or feedback can be submitted using the Online form available at the Contact us page.

This record of processing activity relates to the processing of the name (including title), contact information (email address, postal address, location information, telephone numbers) and, if needed, the application number(s) of EPO customers filing a complaint. This record of processing activity explains the way in which the above personal data are handled.

Purpose of Processing Users of the Patent system can submit

Complaints and feedback are forwarded to a dedicated EPO department responsible for
(i) ensuring that the complaint/feedback is dealt with fairly and efficiently and that suitable measures are taken to address it; and
(ii) providing a comprehensive reply.

If a complaint relates to file-specific substantive or procedural issues, it will usually first be discussed with the relevant internal stakeholders (e.g. managers of the department in charge of the application, or the examining or opposition division). Subsequently, a detailed reply is sent to the complainant, see also Guidelines for Examination in the European Patent Office E VI, 4

The complaint/feedback handling procedure does not replace the procedures laid down by the European Patent Convention; nor does the department responsible for handling complaints/feedback take decisions on substantive and procedural requests. Hence, the relevant department competent for the respective proceedings decides on:
a) complaints/feedback relating to procedural and/or substantive aspects of specific pending proceedings which are submitted by a party to said proceedings. All parties to the proceedings will be informed accordingly.
b) Complaints/feedback relating to substantive issues which are submitted by a third party while proceedings are pending before the EPO. Such a submission will be treated as a third-party observation. (see Guidelines for Examination in the European Patent Office E VI, 3).

The department responsible for handling complaints/feedback promptly forwards any complaint/feedback relating to appeal proceedings to the EPO Boards of Appeal Unit.

Complaints/feedback having a substantive and/or procedural bearing on proceedings before the EPO, as well as replies thereto by the department responsible for handling complaints/feedback, will only exceptionally be excluded from file inspection (see Guidelines for Examination in the European Patent Office D II, 4.3; decision of the President of the EPO concerning documents excluded from file inspection, OJ EPO 2007, Special edition No. 3, J.3).

In general, replies to complaints/feedback are sent as email or attachment to email via the address support@epo.org.

Personal data are processed solely for the purpose of accurately identifying a complainant and sending a reply to their email or postal address provided in the submission of a complaint or feedback.

The processing is not intended to be used for any automated decision-making, including profiling. Personal data will not be transferred to recipients outside the EPO.

complaints or feedback using an electronic form which is available at the EPO website via the Formal complaint / feedback form link in the "Contact us" page of the EPO website. Complaints or feedback may also be submitted via a telephone call to the First Line Customer Enquiries Unit (1LCEU) or by sending a letter addressed to the EPO, to the President, to a Vice-President or to a Director. A case is always created and registered in a database, currently ServiceNow, a registration number in the form "CS123456" is generated, and the case is assigned to the "External Complaints" group of PD15 and PD13 for further processing. Once a case is registered as a complaint or feedback, an automated acknowledgement of receipt is sent to the user by email. Processing of the complaint or feedback includes the steps of analysing the user's input, contacting the department dealing with the corresponding service, dialogue with regard to the root cause of the possible issue, and compiling a reply to the user within 20 days of the date of submission of the complaint or feedback.

Data Retention A patent provides a legal protection for 20 years, and there is no limitation to how long the post-grant procedures can last: after the patent granting procedure, there can be an opposition procedure which will review the patent granting procedure and involve members of the examining division. These members need to be able to retrieve their actions and comments. Moreover, after the patent granting procedure, there may be an appeal procedure whose outcome can be to reopen the examination procedure by the examining division. After that, revocation and limitation procedures may take place at any time, even after expiry of the patent protection. The examining division needs to be able to retrieve the actions and comments of the initial procedure. For more information, see the Decision of the President of the European Patent Office dated 13 December 2021 pertaining to the processing of personal data in patent-grant and related proceedings (OJ EPO 2021 A98). Personal data used which are part of the patent grant procedure are stored indefinitely. If considered appropriate, other personal data (for example names of administrative staff of a representative that process submissions made in MyEPO Portfolio) may be deleted if it can reasonably be expected that there is no operational need anymore, with a maximum of 10 years. In the event of a formal appeal/litigation, all data held at the time the formal appeal/litigation was initiated will be retained until the proceedings have been closed.

As a rule, in case of a complaint, a copy of the complaint form and the reply will be included in the public part of the file. However, the principles governing exclusion from file inspection apply to the complaints/feedback procedure. This means, in particular, that parts which could be prejudicial to the legitimate personal or economic interests of a natural or legal person can be excluded from file inspection at your request or ex officio by the EPO. In such case, contact details will be stored for five years after they have been used or updated the last time, i.e. after the last interaction with the data subject within the framework of Customer Service Management. Personal data received with an enquiry will be anonymised five years after the closure of a particular ticket, allowing the anonymised data to be used for statistical purposes.

When a complaint or feedback is not related to a file, the retention period and anonymisation of the previous paragraph apply.

Data subjects and categories of personal data

Externals

Phone Call Information	
Caller's Phone Number	
Contact Information	
Contact Details	Home Address
Mobile Phone Number	Personal Email
Phone Numbers	Private Phone Number
Working email address	
Patent Process Related Data	
Personal data potentially included within the content of patent procedure related information and publications	

Employment Information	
Company Entity	Office Location
Personal Identification	
First Name	Full Name
Gender	Surname

Recipient of the personal data

Recipients of the data Access to the database with the personal data of users submitting a complaint or feedback is strictly limited to the persons in PD1.5 & PD 1.3 dealing with the complaint.

Personal data might be disclosed on a need-to-know basis to the EPO staff working in DG0, DG1, DG4 and DG5, including the concerned staff member(s).

Personal data are not disclosed to third-party service providers for any maintenance and support purposes.

Personal data will only be shared with authorised persons responsible for the necessary processing operations. They will not be used for any other purposes or disclosed to any other recipients.

Purpose of sharing Processing of the complaint or feedback includes the steps of analysing the user's input, contacting the department dealing with the corresponding service, dialogue with regard to the root cause of the possible issue, and compiling a reply to the user within 20 days of the date of submission of the complaint or feedback.

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 438

Name Digitisation of incoming paper documents, paper file related internal tasks and preparatory work for DG1 formalities officers

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 46 - CIO / BIT

Entity Name - Controller (Entities) DG1 - 11 - COO

External processors

SPS

External processors	
Name SPS	

Description of the processing

Description The processing relates to digitisation of incoming paper documents, paper file related internal tasks and preparatory work for formalities officers. The purpose of the processing is to make incoming patent related documents available in the EPO's electronic dossiers. In proceedings before the EPO, documents may be filed by hand, by postal services or by means of electronic communication.

The EPO confirms the receipt of newly filed applications by sending an acknowledgement of receipt. Paper filed documents are received in the EPO Logistics Centres in The Hague or Munich. The Logistics Centre staff sorts out the documents. Patent related mail is sorted per date of receipt, put into boxes and delivered to the external processor of the particular service group for further treatment. The scanning is done using EPO hardware and software. The documents are scanned into the electronic file according to detailed instructions. After scanning, the original paper documents are stored in boxes in order to be archived.

During the preparatory work, starting from cut-open envelopes delivered from the messenger service or electronic requests to scan an old original paper file, paper files are sorted into three categories: new applications, subsequently filed documents (SFDs) and others. A date stamp is provided on the first page.

The paper documents are sorted per application including indexing sheets ready for indexing and bundled empty envelopes ready for storage for one year. Where necessary, receipts of documents are provided ready for dispatch.

A paper package with completed index or package data sheet (PDS) on top are finalised into packages and fed in batches into a scanner. Thus, the data is loaded in the system, and the paper batches are boxed for on-site storage. The boxes are transported to short-term storage area on the EPO premises and placed on shelves.

Labels and barcodes attached to the boxes and an electronic documentation allow to retrieve an original document from a batch following a request from the EPO for rescanning, for missing documents or for forwarding originals.

After 1 – 2 months on-site storage, the process of off-site storage of patent grant process (PGP) paper files is initiated.

Receipt of patent related data stored on a data carrier (e.g. CD, DVD, diskette, USB sticks, virtual drive, etc.) comprises definition of the loading software and the target EPO database after a virus check run and identification of which data need to be loaded and load them into the defined target EPO database and handing data carriers back to EPO.

The File Management Team in The Hague deals with the incoming e-mails with third party observations (3PO) are assigned to the file concerned and uploaded to the respective file management tool.

Requests for rescanning an original document are performed by retrieving the original file, rescanning the respective documents and loading the rescans in the file management tool.

For paper files in the off-site storage (central file store), which meet the DG1 destruction criteria and legal retention policy, a list is provided to the external processor. The files are then retrieved, listed as becoming obsolete in the contractor and EPO tool and put for destruction.

The agreement also includes indexing and scanning of DG5 PGP-related documents and application cases. Batches of original documents are made available by DG5, indexed, scanned and OCR-processed by the external processor and sent back to DG5.

A further task performed by the File Management Team in The Hague consists of manually amending the bibliographic data of published international applications in the data processing system of the EPO as, after being transmitted on-line from WIPO (World Intellectual Property Organization), certain data cannot be converted automatically. It includes creating, checking, re-formatting and/or updating applicants' and/or inventors' addresses. Processed PCT application numbers are uploaded in EPASYS and/or for exceptional cases, a partly processed application is returned to the EPO for final processing.

A further task performed by the File Management Team in The Hague consists of matching addresses (applicant, postal or representative addresses) with the existing addresses in CDS (Client Data System). When new applications (PCT/ISA, PCT/RO, EP-OLF, EP-paper,) are received at the EPO, an internal tool, Python, tries to match the received addresses with existing ones in CDS without human intervention. When the tool does not find a 100% match, a matching request is sent to SPQR. The addresses are grouped per procedure as the matching criteria are slightly different per procedure (data entry rules for addresses at the EPO).

An address matched by the File Management Team in The Hague is sent automatically to the EPO internal tool, Python, for further

Purpose of Processing The purpose is to make incoming patent related documents available in in the EPO's electronic dossiers. In proceedings before the European Patent Office, documents may be filed by hand, by postal services or by means of electronic communication. If required, the EPO confirms the receipt of patent related documents by sending an acknowledgement of receipt. Paper filed documents are received in the EPO central mailrooms in The Hague or Munich. The mailroom staff sorts out the documents. Patent related mail is sorted per date of receipt, put into boxes and delivered to the Contractor of the particular service group for further treatment. The scanning is done using EPO hardware and software. The documents are scanned into the electronic file according to detailed instructions. After scanning the original paper documents have to be stored in boxes in order to be archived. The Contractor shall also handle incoming faxes which are received at the central fax server and need to be dealt with within short timeframes. The faxes are checked on completeness, content and legibility and transferred to the electronic dossier., The purpose of the processing is to make incoming patent related documents available in the EPO's electronic dossiers. In proceedings before the EPO, documents may be filed by hand, by postal services or by means of electronic communication. The EPO confirms the receipt of newly filed applications by sending an acknowledgement of receipt. Paper filed documents are received in the EPO Logistics Centres in The Hague or Munich. The Logistics Centre staff sorts out the documents. Patent related mail is sorted per date of receipt, put into boxes and delivered to the external processor of the particular service group for further treatment. The scanning is done using EPO hardware and software. The documents are scanned into the electronic file according to detailed instructions. After scanning, the original paper documents are stored in boxes in order to be archived. During the preparatory work, starting from cut-open envelopes delivered from the messenger service or electronic requests to scan an old original paper file, paper files are sorted into three categories: new applications, subsequently filed documents (SFDs) and others. A date stamp is provided on the first page.

processing or a partly processed application is returned to the EPO for final processing.

Another task consists of visually checking on screen all pages of EP application documents to ensure that certain formal requirements are met. Since 1st of April 2024, this task is performed by Formalities Officers in DG1 Directorates.

The last task done on-site by the external processor under Logistics Centre in The Hague consists of finalising certified copies printed by the EPO. The certified copies are added to empty wrappers. The wrappers are bound, and any necessary elements are added. All contents are packaged (e.g. envelope or other) and placed in the out tray ready for sending out to the external recipients/customers.

Data Retention Personal data will be kept only for the time needed to achieve the purposes for which it is processed.

Personal data will be deleted after 5 years.

In the event of a formal appeal/litigation, all data held at the time the formal appeal/litigation was initiated will be retained until the proceedings have been closed.

Data subjects and categories of personal data

Externals

Contact Information	
Contact Details	Country
Home Address	Mobile Phone Number
Personal Email	Phone Numbers
Private Phone Number	Working email address
European Patent Register Data	
Address	Data provided by the data subjects
Correspondence	
Additional Information which might be provided in the course of exchanges	Personal information provided voluntarily
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of a patent (claims, description, drawings, abstract)
Personal data potentially included within the content of patent procedure related information and publications	
Personal Identification	
First Name	Full Name

Surname	

Employees

Contact Information	
Phone Numbers	
Employment Information	
Business Unit Division	
Personal Identification	
First Name	Full Name
Surname	

Recipient of the personal data

Recipients of the data Personal data are processed under the responsibility of DG 1's PD – 1.1 - COO Operations, acting as the EPO's delegated data controller.

Personal data are processed by the EPO staff involved in managing the processing activity referred to in this statement.

External contractors involved in the processing activity may also process personal data, which can include accessing it.

The data is received by the employees of the contractor. They perform their duties on-site at the EPO premises.

The external processor is under the Logistics Centre responsibilities in The Hague and Munich. The Location of the external processors are on-site at the EPO premises in The Hague and Munich.

EPO staff of Directorate 1195 (File Management & Publications – TH / File Management & CDR – MU) interacts with the contractor under Logistics Centre TH and MU.

Purpose of sharing Personal data are processed by the EPO staff involved in managing the processing activity.

External contractors involved in the processing activity may also process personal data, which can include accessing it.

The data is received by the employees of the contractor. They perform their duties on-site at the EPO premises.

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, All personal data are stored in secure IT applications in accordance with the EPO's security standards. Appropriate levels of access are granted individually only to the above-mentioned recipients. For systems hosted on EPO premises, the following basic security measures generally apply: User authentication and access control (e.g. role-based access control to the systems and network, principles of need-to-know and least privilege) Logical security hardening of systems, equipment and network Physical protection: EPO access controls, additional access controls to datacentre, policies on locking offices Transmission and input controls (e.g. audit logging, systems and network monitoring) Security incident response: 24/7 monitoring for incidents, on-call security expert. In principle, the EPO has adopted a paperless policy management system; however, if paper files containing personal data need to be stored on EPO premises, they are locked in a secure location with a restricted access. External providers processing the personal data have committed in a binding agreement to comply with their data protection obligations under the applicable data protection legal frameworks.

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 440

Name EPO outreach activities

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 45 - CTO / BIT

Entity Name - Controller (Entities) DG1 - 15 - Customer Journey and KAM

Description of the processing

Description This record of processing activity refers to the outreach activities carried out by the Customer Journey directorate. Customer Journey helps users get the best customer experience in their interaction with the EPO by
• reaching out proactively
• providing Key Account Management services
• solving enquiries
• supporting Customer Engagement
• monitoring the Customer Enquiries resolution
• coordinating User Satisfaction surveys
• administering complaints
• monitoring Customer Intelligence data coming from user interactions

The Customer Journey directorate focuses on business intelligence, contacts and relations with key users, promoting new services and tools, offering online services training and user days as well as tailor-made workshops and market research. It also organises workshops and conferences in cooperation with units across the EPO. The latest customer outreach activities include meetings with key users from industry.
Dedicated meetings with SMEs and private applicants are offered as well to meet the specific needs of this user segment.

The data processed by Customer Journey derives partly from the Customer Services Management (CSM) tool as defined in the corresponding data protection statement on https://www.epo.org/en/about-us/office/data-protection-and-privacy under "Information on the processing of personal data in EPO products and services" under "For the management of interactions with users contacting the EPO", item 8.
Additional data can also be drawn from the BIT and DG4 Corporate Services databases regarding the use of EPO online services.

This record of processing activity focuses on the outreach activities where staff from the Customer Journey directorate contact customers

in a proactive way. These activities include:
1. promoting large scale events aimed at informing users of the latest developments at the EPO, such as the EPO User Day, by contacting EPO users (data subjects),
2. promoting events related to EPO Online Services to inform users of the latest developments, how to best use the EPO Online Services, collect feedback and reply to questions, by contacting EPO users (data subjects),
3. promoting workshops on specific relevant topics such as the latest developments of EPO tools or services or legal changes, targeted to specific users by contacting these specific users (data subjects),
4. contacting users to solicit feedback on EPO Online Services,
5. informing users on relevant information related to the EPO Online Services,
6. informing users on relevant information related to the EPO's user outreach activities.

Persons who can be contacted include:
1. individuals who have contacted the EPO for enquiries, have their contact details stored in the EPO customer database and have not objected to receiving further communications from the EPO,
2. individuals who have registered for a previous EPO event and who have not objected to receiving further communications from the EPO,
3. Users (i.e. companies, applicants or patent attorney firms) of the following services:
• MyEPO Portfolio services
• Online Filing 2.0 service
• 'Legacy' online services such as eOLF
• EPO smart card

To achieve this purpose, the EPO sends an e-mail to the users providing the relevant information via an external mailing tool or via an e-mail from an EPO employee.

Personal data will not be transferred to recipients outside the EPO which are not covered by Article 8(1), (2) and (5) DPR unless an adequate level of protection is ensured. In the absence of an adequate level of protection, a transfer can only take place if appropriate safeguards have been put in place and enforceable data subject rights and effective legal remedies for data subjects are available, or if derogations for specific situations as per Article 10 DPR apply.

Data Retention Personal data will be kept only for the time needed to achieve the purposes for which it is processed.

Personal data processed for this purpose will be deleted five years after the date of collection.

In the event of a formal appeal/litigation, all data held at the time the formal appeal/litigation was initiated will be retained until the proceedings have been closed.

Purpose of Processing The Customer Journey directorate focuses on business intelligence, contacts and relations with key users, promoting new services and tools, offering online services training and user days as well as tailor-made workshops and market research. It also organises workshops and conferences in cooperation with units across the EPO.

Data subjects and categories of personal data

Externals

Contact Information	
Contact Details	Home Address
Personal Email	Working email address
European Patent Register Data	

Address	
Device Management Data	
Account ID	
Employment Information	
Company Entity	
Personal Identification	
Full Name	

Recipient of the personal data

Recipients of the data Recipients are the EPO staff working in the Customer Journey directorate.
Personal data may be disclosed to third-party service providers for support purposes.

Purpose of sharing Personal data are disclosed on a need-to-know basis to the EPO staff working in the Customer Journey directorate.

Personal data may be disclosed to third-party service providers for support purposes.

Personal data will only be shared with authorised persons responsible for the necessary processing operations. They will not be used for any other purposes or disclosed to any other recipients.

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 441

Name Procurement activities

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG4 - 47 - Procurement and Vendor Management

External processors

iValua

External processors	
Name iValua	

SAP

External processors	
Name SAP	

DocuSign

External processors	
Name DocuSign	

DocuSign

External processors

Name
DocuSign

AI - Administration Intelligence

External processors
Name
AI - Administration Intelligence

Description of the processing

Description Companies intending to submit a bid to EPO tenders need to register a user profile on the EPO's eTendering platform. At this occasion a valid business email address must be provided, together with contact details.

Once registered, companies can use the eTendering platform to download procurement documents and enter effectual bids and submit legally valid electronic offers. Offers may contain personal data provided by the company/bidder such as names, contact details, and CVs of employees.

PD47 processes the data via the eTendering platform to communicate with the bidding companies and to carry out tender procedures.

After winning a bid and a contract, new suppliers need to register to sign up to the EPO procurement and sourcing portal which has been designed to improve partnership and transparency and optimise co-operation between the EPO and its suppliers. During this registration, in addition to company data, an employee of the supplier needs to be assigned for contact purposes and respective data (name, contact details) are to be provided. Contract conclusion involves contract signing electronically via DocuSign integration.

Registered suppliers can use the EPO procurement and sourcing portal to maintain and update the company data and contact details. Additionally, new or amended contracts can be signed or viewed.

PD47 processes the data via the EPO procurement and sourcing portal for concluding contracts and carrying out purchasing activities with suppliers.

In addition to the above, PD47 maintains an overview of currently active and planned direct placement or tender procedures in Excel (the only personal data included here is the name of the responsible buyer) and an archive with all relevant information on procurement activities via direct placement or tender procedures in the document management system of the EPO.

On a need-to-know basis, personal data (name, contact details) are made available to Legal (contract conclusion) or Finance (purchasing activities).

Data Retention Personal data processed for the verification of the identity in the context of the e-signature are retained for a maximum of 90 days before being erased.

Personal data processed during procurement activities will be kept for 12 years

Purpose of Processing manage and carry out procurement activities

Data subjects and categories of personal data

Externals

Contact Information

Contact Details	Working email address
Correspondence	
Additional Information which might be provided in the course of exchanges	
Employment Information	
Job Title Role	
Personal Identification	
Digital signature	Full Name
Signature	
User Account Information	
Account Password	User ID
System Logs	
System-, Application-, Security-related Server Logs	
Government Identifiers	
ID/Passport picture	National Identity Card Details

Employees

Contact Information	
Contact Details	
Employment Information	
Job Title Role	
Personal Identification	
Digital signature	Full Name
System Logs	
System-, Application-, Security-related Server Logs	

Recipient of the personal data

Recipients of the data PD41 Finance and PD52 Legal

Purpose of sharing

Transfer

Transfer Yes

Country where data might be transferred - Processor (Vendors) SAP - Germany, DocuSign - United States

Transfer to public authority and/or International Organisation

Transfer mechanism(s) Explicit consent of the data subject, The recipient provided appropriate safeguards

Reasons for the transfer DocuSign is the service provider for the electronic signature solution

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 443

Name Legal Business Partner brand

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG5 - 52 - Legal Affairs

External processors

Microsoft

External processors	
Name Microsoft	

Description of the processing

Description PD Legal Affairs serves as a centre of excellence for the provision of legal analysis, assistance and advice in legal matters with a strategic, policy, institutional or external dimension. We aim at consistent delivery of legal service and ensuring the highest levels of quality and timeliness.

In this context, to provide for senior management a real-time overview of ongoing cases dealt with in Legal Affairs, PD52 makes available to them a spreadsheet with basic information on each case (such as lawyer(s) involved, subject matter) and associated legal risk evaluation.

The processing is not intended to be used for any automated decision-making, including profiling.

PD Legal Affairs serves as a centre of excellence for the provision of legal analysis, assistance and advice in legal matters with a strategic, policy, institutional or external dimension. We aim for a consistent delivery of legal service and ensuring the highest levels of quality and timeliness.

In this context, to provide senior management with a real-time overview of ongoing cases dealt with in Legal Affairs, PD52 makes a spreadsheet available to them with basic information on each case (such as lawyer(s) involved, subject matter) and associated legal risk evaluation.

The processing is not intended to be used for any automated decision-making, including profiling.

Purpose of Processing - Defining and documenting roles and responsibilities - Streamlining legal risk management - Enhancing transparency towards stakeholders ensuring that senior management is informed about which colleagues are responsible for specific cases; and - Facilitating exchange and early alignment with Vice-President DG5 and/or the President of the Office in ongoing legal cases dealt by Legal Affairs.

Data Retention Case handlers' and deputies' names are displayed only as long as the associated case is ongoing. Further personal data remaining available on the list of closed cases (e.g. Case management System ticket reference) is deleted at the latest two years after the end of the year in which the case was closed.

In the event of a formal appeal/litigation, all data held at the time the formal appeal/litigation was initiated will be retained until the proceedings have been closed.

Data subjects and categories of personal data

Externals

Matter/Log file	
Metadata	
Ticketing	
Ticket related data	
Professional Experience & Affiliations	
Affiliation	
Employment Information	
Job Title Role	
Personal Identification	

Full Name	

Employees

Matter/Log file	
Metadata	
General	
Any other information	Assessment and legal opinions
Input provided during the deliberation and decision-making process	Legal opinions and assessments
Ticketing	
Ticket related data	
Correspondence	
Any other information	
Employment Information	
Assessment and legal opinions	Business Unit Division
Department name and/or number	
Personal Identification	
Full Name	

Recipient of the personal data

Recipients of the data Performance and Process office,
Vice-President DG5 office
Possibly President's office also

Purpose of sharing The sharing of this information with hierarchy is the purpose of the legal business partner model

Transfer

Transfer No

Country where data might be transferred - Processor (Vendors)
Microsoft - United States

Transfer to public authority and/or International Organisation

Reasons for the transfer

Transfer mechanism(s)

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 446

Name Patent Index

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG0 - 02 - Communication, DG1 - 15 - Customer Journey and KAM

Entity Name - Controller (Entities) DG0 - 02 - Communication

External processors

Microsoft

External processors	
Name Microsoft	

Microsoft

External processors	
Name Microsoft	

Description of the processing

Description As part of the annual Patent Index, the EPO publishes rankings for Top Applicants for the previous calendar year, for selected countries and also in the leading ten technical fields.
Although this data is derived from patent applications that may content personal data, personal data is only used for the preparation of statistics, whereas the anonymous statistics are then published in the Patent Index.
To ensure the accuracy of the rankings, the Chief Business Analyst unit operates a "scope of consolidation exercise" in which the leading 150-200 companies and research organisations, for patent applications to the EPO in the previous year, are contacted individually and asked to confirm that the way in which we count applications in respect of their company or group is correct.
The list of the provisional Top 150-200 applicants for the current year (i.e. the year on which the President Index will report the following March) is based on the process of consolidation from previous years, EPO databases, and publicly available information. PD Communication receives therefore a contact list database in the form of a spreadsheet from DG1 1 5, which contains the contacts of 150-200 key account IP managers from the firms that have filled the most applications to the EPO. E-emails are sent from a dedicated mailbox to which only four people have access, only from PD Communication and the User Intelligence Unit from DG1.
The exercise gives these major customers the chance to explain to us which of the entities in their group should have their patent applications tallied together under one company or group, or which should be counted separately. Therefore, additional personal data may be collected and processed during the email exchanges. Nevertheless, the used of this personal data is limited to the confirmation of the data and ranking that is finally published.
The data collected by PD Communication is stored in an internal SharePoint database for the relevant retention period. The files are then deleted and updated with the new files provided by DG15 for the next annual Patent Index exercise.
The processing operation is partially automated. It is based on an exchange of Excel sheets and email exchanges among EPO internal organisational units and between the EPO and relevant key account IP managers. No paper files are used as part of this processing operation.

Data Retention Personal data will be kept only for the time needed to achieve the purposes for which it is processed.
For personal data related to contact details (e.g.: name, surname, email address, affiliation) they are stored for and deleted after a maximum period of 2 years as part of an internal EPO contact details database owned by PD Communication.

Purpose of Processing publication of patent-related statistical data., The personal data are processed by PD 02 for the purpose of verifying the top 100 applicants in the Patent Index for the year in question.

Data subjects and categories of personal data

Externals

Contact Information	
Contact Details	Country
Home Address	Personal Email
Phone Numbers	Working email address
European Patent Register Data	
Data provided by the data subjects	
Correspondence	

Personal information provided voluntarily	
Patent Process Related Data	
Personal data potentially included within the content of a patent (claims, description, drawings, abstract)	Personal data potentially included within the content of patent procedure related information and publications
Employment Information	
Job Title Role	Office Location
Personal Identification	
First Name	Full Name
Surname	

Recipient of the personal data

Recipients of the data The personal data are disclosed to specific members of the EPO staff working in PD Communication and DG1 (DG 15) and the PD Communication team working on the creation and distribution and promotion of the Patent Index.

Purpose of sharing The personal data are disclosed to specific members of the EPO staff working in PD Communication and DG1. The personal data can only be accessed on a restricted basis and only for the purposes of verifying the top 100 applicants of the Patent Index.

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards, Data Protection EU Comm Standard Contractual Clauses

Country where data might be transferred - Processor (Vendors) Microsoft - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 457

Name Personal data collected in the context of building projects for obtaining Building Permits at EPO Sites

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 44 - General Administration

Entity Name - Controller (Entities) DG4 - 44 - General Administration

Description of the processing

Description To obtain building permits at an EPO site, all affected neighbors must be notified about the planned changes detailed in the building permit application. Legal approval from these neighbors is necessary for the permit to be granted. If applicable, the municipalities of EPO sites will provide a list of addresses for all neighbors who need to be notified.

Previously, signatures from neighbors were required on all building plans, which are stored within the EPO network. If the EPO, as a neighbor, is asked to approve a neighbor's building permit, the related documents are used only internally and stored securely within our cloud or server to ensure confidentiality and data integrity.

During the execution phase of a project, direct contact with neighbors may be necessary. In such cases, personal data such as mobile numbers must be stored by the project manager, who is responsible for ensuring this data is stored securely and accessed appropriately.

Data Retention Personal data are collected to obtain building permits which are kept 50 years. But the personal data are anonymised once the project has been finalised and before the documents are stored for archiving purposes.

Purpose of Processing To obtain building permits at an EPO site, all concerned neighbors must be informed about the the planned changes within the EPO building, as outlined in the building permit application. Legal approval from these neighbors is required for the permit to proceed. When applicable, the municipalities of EPO sites provide a list of addresses for all neighbors who need to be informed. In cases where the EPO is a neighbor and is required to approve a neighbor's building permit, the related documents are used solely for internal purposes. These documents are securely stored within our cloud or server infrastructure to maintain confidentiality and data integrity. For direct contact with neighbour during the execution phase of a project, personal data like mobile numbers have to be stored by the project manager. The project manager is responsible for ensuring that this personal data is stored securely and accessed appropriately.

Data subjects and categories of personal data

Externals

Contact Information	
Home Address	Mobile Phone Number
Personal Email	Phone Numbers

Working email address	
Personal Identification	
Full Name	Signature

Recipient of the personal data

Recipients of the data Buildings permits (including plans) are shared with external planners, consultants and/or contractors but not processed by them. The later are bound to a confidentiality clause in their contract).

Purpose of sharing Buildings permits (including plans) are shared with external planners, consultants and/or contractors in order to work on the building project with EPO project managers.

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 458

Name PGP paper files in C-Lab

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG4 - 4 - Corporate Services

Description of the processing

Description The record relates to the handling of personal data in the context of exhibiting a sample of several thousands of patent grant process (PGP) paper files in the EPO's Culture Space A&T5-10 (C-Lab). The storage is part of a broad initiative to preserve and showcase the historical and artistic heritage of the EPO in a secure exhibition.

Data Retention Personal data will be kept for the 60 years, in line with the retention period set for the paper PGP files concerned in the EPO Documentation Policy.

Purpose of Processing Exhibition of a sample of PGP paper files in the A&T 5-10 Culture Space

Data subjects and categories of personal data

Externals

Contact Information	
Country	Home Address
Personal Email	Phone Numbers
Working email address	
Personal Identification	
First Name	Full Name

Employees

Personal Identification

First Name	Full Name
Surname	
User Account Information	
User ID	

Former Employees

Personal Identification	
First Name	Full Name
Surname	

Recipient of the personal data

Recipients of the data As a general rule, personal data will not be shared with any recipient. Visitors of the exhibition are not allowed to access the files and the personal data contained therein.

Purpose of sharing

Transfer

Transfer No

Country where data might be transferred - Processor (Vendors)

Transfer to public authority and/or International Organisation

Reasons for the transfer

Transfer mechanism(s)

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures Instructions are in place that do not allow visitors and/or other individuals to access the files and the personal data contained therein.

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 460

Name Management of personal data in building permit applications

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 44 - General Administration

Entity Name - Controller (Entities) DG4 - 44 - General Administration

Description of the processing

Description For the purpose of obtaining building permits at a given EPO site, all neighbors concerned need to be informed and their approval is legally required if relevant changes within the building are planned and described in the building permit. If applicable, the municipalities of EPO sites send a list of all neighbours' addresses.
In cases where the EPO is a neighbor and is required to approve a neighbor's building permit, the related documents are used solely for internal purposes. These documents are securely stored within our cloud or server infrastructure to maintain confidentiality and data integrity.
For direct contact with neighbour during the execution phase of a project, personal data like mobile numbers have to be stored by the project manager. The project manager is responsible for ensuring that this personal data is stored securely and accessed appropriately.

Data Retention Building permits are kept 50 but personal data are anonymised as soon building permits are obtained.

Purpose of Processing To obtain buidling permits from the municipality (ies)

Data subjects and categories of personal data

Externals

Contact Information	
Home Address	Mobile Phone Number
Personal Email	Working email address
Personal Identification	
Full Name	

Recipient of the personal data

Recipients of the data EPO staff to contact the neighbors for permits obtention and contractors in charge of the project see the information on the documents.

Purpose of sharing To contact the neigbors to get their approval for the building permit.

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 462

Name EPO Legal Interactive Platform

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG4 - 45 - CTO / BIT

External processors

Microsoft

External processors	
Name Microsoft	

Google Ireland Limited

External processors	
Name Google Ireland Limited	

Microsoft

External processors	
Name Microsoft	

Description of the processing

Description The present processing operation pertains to the processing of personal data done in the scope of the EPO Legal Interactive Platform, which is a service offered to selected MyEPO.org users as an option in their portfolio of functionalities.
The EPO Legal Interactive Platform is an EPO chatbot which empowers users to guide conversations towards specific levels of detail on subjects related to legal topics within the legal sources listed below. Through successive prompts and replies, users can fine-tune the context of their discussions. To facilitate users returning to prior conversations, the Legal Interactive Platform retains the history of interactions for each user; users can permanently delete own past interaction history at any time. The user can express an opinion in the form of a feedback regarding the quality of the answer received and in case of negative feedback he is allowed to include a feedback comment to help improving the tool. Feedback, both positive and negative, will be used for further tuning and improvements.
The tool is designed to provide information and answer questions specifically about the European Patent System.
Users of the EPO's Legal Interactive Platform are invited to enter in the chatbot's prompts exclusively information that is available in the public domain.

Data Retention Logs are kept for up to three months.
Users' chat history is kept for up to three years; the user has the ability to delete it at any time.
User feedback is retained for up to three years.

Purpose of Processing The processing operation consists in collecting and sending the user's prompts entered into the chatbot's user interface and in storing the user's past chat history into a database (hosted on Azure Cloud) along with the User ID which has been hashed and truncated. Prompts that do not lead to a completion (i.e. to an answer from the LLM - Large Language Model) are not stored in the database; all other prompts are stored with the User ID hashed and truncated exclusively to enable retrieval. The purposes of processing are: • to answer user's queries about the European Patent System, also by means of user's subsequently refined prompts; • to facilitate the user carrying on a conversation with the chatbot by retaining and leveraging the user's past interaction history; • to improve the accuracy of EPO's Legal Interactive Platform service by analysing the saved prompts; the user ID of the user who has entered a given prompt and/or feedback is pseudonymised by means of hashing and truncation; • to identify, troubleshoot and fix anomalies and incidents affecting the service; • to derive anonymised statistics about most searched topics. The processing is not intended to be used for any automated decision-making, including profiling.

Data subjects and categories of personal data

Externals

General	
User's prompts	
Network/application Interaction Data	
Session content	Session details
Session metadata	
Sensory and Electronic Information	
Audio Information	
Correspondence	
Chat content	Feedback received
Browsing Information	
Browser User Agent	Browsing Date and Time
Cookie Information	IP Address
User Account Information	
User ID	
System Logs	

System-, Application-, Security-related Server Logs	Web Servers Logs

Recipient of the personal data

Recipients of the data Personal data are shared on a need-to-know basis to these recipients:
- BIT 4513 Data scientists, for the purpose of analysing users' prompts, feedback and comments;
- BIT 45323 Patent Work Bench product team, for maintenance of the service;
- to Microsoft (cloud service provider), for the delivery of the service.

Purpose of sharing Personal data are shared to:
- DG4 BIT Data scientists, for the purpose of analysing users' prompts, feedback and comments;
- DG4 BIT Patent Work Bench product team, for maintenance of the service;
- Microsoft (cloud service provider), for the delivery of the service.

Transfer

Transfer Yes

Country where data might be transferred - Processor (Vendors) Microsoft - United States, Google Ireland Limited - Hong Kong, Google Ireland Limited - Taiwan, Google Ireland Limited - Brazil, Google Ireland Limited - Qatar, Google Ireland Limited - Indonesia, Google Ireland Limited - Singapore, Google Ireland Limited - Malaysia, Google Ireland Limited - Saudi Arabia, Google Ireland Limited - United States, Google Ireland Limited - Philippines, Google Ireland Limited - India, Google Ireland Limited - Australia, Google Ireland Limited - Chile

Transfer to public authority and/or International Organisation

Reasons for the transfer Protection against malware, login to Azure Active Directory, error analysis, load balancing, diagnostics data and processing for Microsoft's business operations.

Transfer mechanism(s) The recipient provided appropriate safeguards

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums)., MyEPO.org users are identified and authenticated via EPO's Customer Identity and Access Management system (CIAM). Masking: UserIDs are hashed and truncated to prevent reidentification

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 463

Name Workflow, Data and Knowledge management based on EPO ServiceNow capabilities

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG4 - 46 - CIO / BIT

External processors

ServiceNow Inc. (USA)

External processors	
Name ServiceNow Inc. (USA)	

Axians

External processors	
Name Axians	

ServiceNow

External processors	
Name ServiceNow	

Description of the processing

Description ServiceNow is a cloud-based platform that offers a suite of services for automating and managing business processes across various departments within an organization.
It provides tools for IT service management, IT operations management, and IT business management, enabling companies to streamline their workflows, enhance efficiency, and improve service delivery.
ServiceNow's platform is designed to be flexible and scalable, allowing businesses to customize and extend its capabilities to meet their specific needs. It integrates with other systems and data sources, offering a centralized solution for managing tasks, incidents, problems, changes, and other IT-related activities.
The platform's user-friendly interface and automation capabilities support a wide range of functions, from simple ticketing to complex enterprise-wide operations.
A virtual agent is natively available in the Service Portal and lets users have an end-to-end conversational experience - with either a bot or a human agent - enabling instant resolution to common IT, HR or customer service requests.

The EPO's ServiceNow platform instances consist of:
-a main set instance, with development, test and production environments
-another set with development, test and production environments, dedicated for the management of the European Qualifying Exam (EQE).

Service Now provides means for a decentralised administration of configuration data with tools provided for users to create their own catalog items (and variables), manage their own workflows etc.
It is therefore possible that personal data of any nature and referred to any data subject could be collected, stored and processed in Service Now - as configured by any user with the required access to administer catalog items and the respective workflows.
It is beyond the scope of the present processing operation to go into the details of which items of personal data or which processing workflows are actually done in EPO ServiceNow. Such information is documented in other RoPAs by the corresponding Delegated Controllers who are accountable for own given processing workflows.

Data Retention Personal data will be kept in EPO ServiceNow only for the time needed to achieve PD4.6 Delegated Controller's purposes and to suit the retention needs and constraints of other EPO Delegated Controllers which use EPO ServiceNow platform.

By default all data is retained in ServiceNow indefinitely, with only a small number of out-of-the box exceptions when it comes to e.g. logging information or temporary records used in the processing of imported data.
The EPO applies a default retention policy of 5 years for all task records and related data; the retention starts upon task closure. Deviations from this default retention policy will be documented in the Record and Statement of the present processing operation unless there is another process-specific Record and/or Statement where any such process-specific deviations should be described.

The CMDB includes a reference to the user to which any given configuration item is assigned only for so long that this is the case. Personal data associated to Knowledge Base articles, articles' ratings and feedback are retained as long as the article's subject matter is valid and applicable to the EPO.

Upon termination or expiration of the Agreement which EPO has signed with Data Processor ServiceNow, ServiceNow shall delete the EPO's data, including personal data contained therein.
In the event of a formal appeal/litigation, all data held at the time the formal appeal/litigation was initiated will be retained until the proceedings have been closed.

Purpose of Processing Delegated Controller PD4.6 processes personal data in EPO ServiceNow for the following purposes: 1. to allow the registration and follow-up of issues, problems and incidents through a ticketing system; 2. to provide a controlled mechanism for the registration and implementation of changes; 3. to permit the logging and execution of requests initiated by end users; 4. to provide an accurate and up-to-date database for software and hardware assets, known as the Configuration Management Database (CMDB); 5. to offer knowledge base management by enabling the given EPO org unit to build own knowledge base; knowledge base articles can be browsed, searched, rated and may receive users' feedback; 6. to perform decentralised administration of any given workflow's configuration data. ServiceNow enables EPO users in creating own catalogue items and variables, manage own workflows etc.; 7. to perform housekeeping tasks required to keep the application and its database operating smoothly and with adequate security; 8. to improve end user's self-service experience and helpdesk productivity via virtual agent chatbot; 9. to permit statistical reporting on tickets and requests and to analyse trends; Processing for purposes 1. to 8. involves personal data whereby individuals can be identified; processing for purpose 9. (statistical reporting) produces anonymised outcomes. No data is extracted from ServiceNow and processed outside it, as the tool already provides a rich reporting interface and dashboarding capabilities.

Data subjects and categories of personal data

Contractors

General	
Any other information	
Ticketing	
Ticket related data	
Contact Information	
Working email address	
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Feedback received
Personal information provided voluntarily	
Personal Identification	
First Name	Surname
User Account Information	
Application Specific User Role	Membership Permissions
User ID	
System Logs	
System-, Application-, Security-related Server Logs	Web Servers Logs

Employees

General	
Any other information	
Ticketing	
Ticket related data	
Contact Information	
Working email address	
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information

Chat content	Feedback received
Personal information provided voluntarily	
Personal Identification	
First Name	Surname
User Account Information	
Application Specific User Role	Membership Permissions
User ID	
System Logs	
System-, Application-, Security-related Server Logs	Web Servers Logs

Externals

General	
Any other information	
Ticketing	
Ticket related data	
Contact Information	
Working email address	
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Feedback received
Personal information provided voluntarily	
Personal Identification	
First Name	Surname
User Account Information	
Application Specific User Role	Membership Permissions
User ID	
System Logs	
System-, Application-, Security-related Server Logs	Web Servers Logs

Former Employees

General	
Any other information	
Ticketing	
Ticket related data	
Contact Information	
Working email address	
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Feedback received
Personal information provided voluntarily	
Personal Identification	
First Name	Surname
User Account Information	
Application Specific User Role	Membership Permissions
User ID	
System Logs	
System-, Application-, Security-related Server Logs	Web Servers Logs

Prospective Employees

General	
Any other information	
Ticketing	
Ticket related data	
Contact Information	
Personal Email	
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Feedback received

Personal information provided voluntarily	
Personal Identification	
First Name	Surname
User Account Information	
Application Specific User Role	Membership Permissions
System Logs	
System-, Application-, Security-related Server Logs	Web Servers Logs

Recipient of the personal data

Recipients of the data Colleagues in BIT 4.6 may have access to personal data in ServiceNow for configuration, operation and maintenance purposes.
Since EPO's Service Now is highly configurable in a de-centralised fashion, any EPO staff member and/or its service providers could potentially be recipients of personal data.

Purpose of sharing Personal data in ServiceNow are shared to intended recipients to enable them performing their specific business tasks on a need-to-know basis.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards, Data Protection EU Comm Standard Contractual Clauses

Country where data might be transferred - Processor (Vendors) ServiceNow - Netherlands

Reasons for the transfer Customer support and incident resolution (e.g. security) purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).,

ServiceNow PHYSICAL SECURITY MEASURES: -DATA CENTER FACILITIES. ServiceNow data centre facilities include (1) physical access restrictions and monitoring that shall include a combination of any of the following: multi-zone security, man-traps, appropriate perimeter deterrents, on-site guards, biometric controls, CCTV and secure cages; (2) fire detection and fire suppression systems both localised and throughout the data center floor. -SYSTEMS, MACHINES AND DEVICES. The systems, machines and devices include (1) physical protection mechanisms; and (2) entry controls to limit physical access. -MEDIA. ServiceNow shall use NIST 800-88 industry standard (or substantially equivalent) destruction of sensitive materials, including Customer Data, before such media leaves ServiceNow's data centers for disposition. ServiceNow TECHNICAL SECURITY MEASURES: -ACCESS ADMINISTRATION. Access to the EPO's ServiceNow by ServiceNow employees and contractors is protected by authentication and authorization mechanisms. User authentication is required to gain access to production and sub-production instances. Individuals are assigned a unique user account. Individual user accounts shall not be shared. Access privileges are based on job requirements using the principle of least privilege access and are revoked upon termination of employment or consulting relationships. Access entitlements are reviewed by management quarterly. Infrastructure access includes appropriate user account and authentication controls, which will include the required use of VPN connections, complex passwords with expiration dates, account lock-out enabled, and a two-factor authenticated connection. -SERVICE ACCESS CONTROL. The ServiceNow service provides user and role-based access controls. The EPO is responsible for configuring such access controls within its instance. -LOGGING AND MONITORING. The production infrastructure log activities are centrally collected, are secured in an effort to prevent tampering, and are monitored for anomalies by a trained security team. ServiceNow shall provide a logging capability in the platform that captures login and actions taken by users in the ServiceNow application. The EPO has full access to application audit logs within own ServiceNow instances, including successful and failed access attempts. The EPO is responsible for exporting application audit logs to Customer's syslog server through available built-in platform features. -FIREWALL SYSTEM. An industry-standard firewall is installed and managed to protect ServiceNow systems by residing on the network to inspect all ingress connections routed to the ServiceNow environment. ServiceNow managed firewall rules are reviewed quarterly. The EPO shall be responsible for reviewing any Customer managed firewall rules on its instances. -VULNERABILITY MANAGEMENT. ServiceNow conducts quarterly security risk evaluations to identify critical information assets, assess threats to such assets, determine potential vulnerabilities, and provide for remediation. When software vulnerabilities are revealed and addressed by a vendor patch, ServiceNow will obtain the patch from the applicable vendor and apply it within an appropriate timeframe in accordance with ServiceNow's then-current vulnerability management and security patch management standard operating procedure and only after such patch is tested and determined to be safe for installation in all production systems. -ANTIVIRUS. ServiceNow updates antivirus, anti-malware, and anti-spyware software on regular intervals and centrally logs events for effectiveness of such software. -CHANGE CONTROL. ServiceNow evaluates changes to platform, applications, and production infrastructure to minimize risk and such changes are implemented following ServiceNow's standard operating procedure. -DATA SEPARATION. Customer Data shall be maintained within a logical single-tenant architecture on multi-tenant cloud infrastructure that is logically and physically separate from ServiceNow's corporate infrastructure. -CONFIGURATION MANAGEMENT. ServiceNow shall implement and maintain standard hardened configurations for all system components within the service subscribed by the EPO. ServiceNow shall use industry standard hardening guides, such as guides from the Center for Internet Security, when developing standard hardening configurations. -DATA ENCRYPTION IN TRANSIT. ServiceNow shall use industry standard encryption to

encrypt EPO's data in transit over public networks to the ServiceNow Service. -DATA ENCRYPTION AT REST. ServiceNow shall provide encryption at rest capability for column level encryption, which the EPO may enable at its sole discretion. -SECURE SOFTWARE DEVELOPMENT. ServiceNow shall implement and maintain secure application development policies and procedures aligned with industry standard practices such as the OWASP Top Ten (or a substantially equivalent standard). All personnel responsible for secure application design and development will receive appropriate training regarding ServiceNow's secure application development practices. -SECURE CODE REVIEW. ServiceNow shall perform a combination of static and dynamic testing of code prior to the release of such code to Customers. Vulnerabilities shall be addressed in accordance with its then current software vulnerability management program. Software patches are regularly made available to Customers to address known vulnerabilities. -ILLICIT CODE. The ServiceNow service shall not contain viruses, malware, worms, date bombs, time bombs, shut-down devices, that may result in, either: (a) any inoperability of the service; or (b) any interruption, interference with the operation of the service. If the service is found to contain any illicit Code that adversely affects the performance of the service or causes a material security risk to EPO's Data, ServiceNow shall, as EPO's exclusive remedy, use commercially reasonable efforts to remove the illicit Code or to advise and assist EPO to remove such illicit Code. ServiceNow ORGANISATIONAL SECURITY MEASURES: -DATA CENTER INSPECTIONS. ServiceNow performs routine reviews of data centers to confirm that the data centers continue to maintain appropriate security controls necessary to comply with its own Security Program. -PERSONNEL SECURITY. ServiceNow performs background screening on all employees and all contractors who have access to EPO's Data in accordance with ServiceNow's then-current applicable standard operating procedure and subject to Law. -SECURITY AWARENESS AND TRAINING. ServiceNow maintains a security and privacy awareness program that includes appropriate training and education of ServiceNow personnel, including any contractors or third parties that may access EPO's Data. Such training is conducted at time of hire and at least annually throughout employment at ServiceNow. -VENDOR RISK MANAGEMENT. ServiceNow maintains a vendor risk management program that assesses all vendors that access, store, process, or transmit EPO's Data for appropriate security and privacy controls and business disciplines. -SOFTWARE AND ASSET INVENTORY. ServiceNow shall maintain an inventory of all software components (including, but not limited to, open source software) used in EPO's ServiceNow service, and inventory all media and equipment where EPO Data are stored. -WORKSTATION SECURITY. ServiceNow shall implement and maintain security mechanisms on personnel workstations, including firewalls, anti-virus, and full disk encryption. ServiceNow shall restrict personnel from disabling security mechanisms. ServiceNow's committments abour own CERTIFICATIONS AND ATTESTATIONS: ServiceNow shall establish and maintain sufficient controls to meet certification and attestation for the objectives stated in ISO 27001, ISO 27018, SSAE 18 / SOC 1 and SOC 2 Type 2 (or equivalent standards) for the Security Program supporting the Subscription Service. At least once per calendar year, ServiceNow shall obtain an assessment against such standards and audit methodologies by an independent third-party auditor and make the executive reports available to the Customer.

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 466

Name RFPSS Recording MS Teams trainings

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities)

Entity Name - Controller (Entities) DG0 - 05 - Administration of Reserve Funds

Description of the processing

Description This data protection statement explains the process used to provide online training as part of implementing the RFPSS Investment Management Platform (Aloha) and the recordings of these session to be made available within the PD Administration of the RFPSS.
General and in-depth training material on Aloha is provided by the service provider, both via video and via an SS&C learning centre. As PD 05 Administration of the Reserve Funds has requested practical training, the intention is to offer hybrid (online and on-site) EPO-specific training in collaboration with external project staff. In order to ensure knowledge is shared and the training information retained, a recording of the training over MS Teams (using the MS Teams recording functionality or a Snagit2023 video recording) is stored in a specific structure in OpenText.
Names, video images and voices are recorded, as these are visible when the training is provided. If a participant in the online training session does not wish their voice of image to be recorded, they can switch off their camera and/or microphone.
The personal data recorded are processed for the following purposes: re-use of the recorded material for participants unable to participate, and future technical reference. The processing is not intended to be used for any automated decision-making, including profiling.

Data Retention The actual recording of the training and any personal data will be deleted after five years.

Purpose of Processing The training - and subsequently the recording of the participants name, voice and video image – are recorded to allow staff which were not present during the presentation to acquainting themselves with the training content at a later stage. Staff which attended the training can use the recording as a fallback of their notes and verify what steps to take in a specific process.

Data subjects and categories of personal data

Contractors

Online invigilation data

Audio input	Webcam captures
Personal Identification	
First Name	Surname

Employees

Online invigilation data	
Audio input	Webcam captures
Personal Identification	
First Name	Surname

Externals

Online invigilation data	
Audio input	Webcam captures
Personal Identification	
Full Name	

Recipient of the personal data

Recipients of the data Staff working in PD 05 - Administration of the Reserve Funds

Purpose of sharing Ensure training material is available to all staff working in PD 05 - Administration of the Reserve Funds

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures	For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 471

Name Deep Tech Finder Application

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 45 - CTO / BIT

Entity Name - Controller (Entities) DG0 - 032 - Chief Economist

External processors

Dealroom

External processors	
Name Dealroom	

Description of the processing

Description The Deep Tech Finder dataset is designed to allow the public to find investment ready start-ups that have patent applications at the EPO. The start-ups database is provided by an external provider located in the European Union and complemented by matched EPO data on published European patent applications.
A Data Protection Agreement (DPA) has been signed with this external provider in which it commits to complying with the EPO Data Protection Rules.

The Office offers an application to customers (external and internal) in order to access this DTF database.

The data which are processed on EPO servers when users access the DTF APP are:.

- the IP address of the end user
- browser user agent
- application traffic for delivering Deep Tech Finder data to the screen

These data are automatically erased 90 days after connection,

The user has access to general information on the DTF APP and the following personal data are processed:

- names and surnames of investors when those investors are individuals
- geographical distribution of the start-ups (mapping)

When the start-up is no longer categorised as such, this data is erased and no longer accessible.

Data Retention End user usage data is retained for 90 days after its first collection. The erasure is done automatically.
App content data is kept for as long as the start-up is categorised as such.

Purpose of Processing Personal data are processed to maintain the basic technical services of the application

Data subjects and categories of personal data

Employees

Browsing Information	
Browser type	IP Address

Externals

Browsing Information	
Browser User Agent	IP Address
Personal Identification	
First Name	Surname

Recipient of the personal data

Recipients of the data The employees of EPO BIT, the Controller and the staff of the Chief Economist Unit get access to the data.
External contractors involved in maintaining the backend services also process the data.

Purpose of sharing Processing is necessary in order to deliver the application features to the user

Transfer

Transfer No

Country where data might be transferred - Processor (Vendors)

Transfer to public authority and/or International Organisation

Reasons for the transfer

Transfer mechanism(s)

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 473

Name Meetings and events managed by PDComm

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG1 - 1 - Patent Granting Process, DG4 - 46 - CIO / BIT, DG4 - 45 - CTO / BIT, DG0 - 02 - Communication

Entity Name - Controller (Entities) DG0 - 02 - Communication

External processors

Slido

External processors	
Name Slido	

SAP

External processors	
Name SAP	

Zoom

External processors	
Name Zoom	

Global Hospitality Platform BV

External processors

Name
Global Hospitality Platform BV

External employees working at EPO in the Principal Directorate Communication.

External processors
Name
External employees working at EPO in the Principal Directorate Communication.

NTT DATA

External processors
Name
NTT DATA

Huddle

External processors
Name
Huddle

Security Services Contractor at all EPO sites

External processors
Name
Security Services Contractor at all EPO sites

Amazon Web Services (AWS)

External processors
Name
Amazon Web Services (AWS)

Microsoft

External processors
Name
Microsoft

Zoom

External processors
Name
Zoom

Description of the processing

Description The present data protection statement describes how the EPO, in particular the Principal Directorate Communication ("PD Communication") processes personal data collected for the purpose of organising and managing on-site and virtual meetings / events / conferences / competitions / trainings / webinars / seminars / broadcasts / campaigns (hereinafter collectively referred to as " meetings/events").

Overall, for all types of meetings/events there are several processing activities that are necessary to organise and manage them. The envisaged processing activities are:

1. Invitations and participation to registration
2. Activities with speakers, panelists and moderators
3. Documentation and promotion
4. Online meeting/event hosting
5. Onsite event hosting
6. Post-event surveys and feedback
7. Cookies and online tracking

Overall, personal data is collected by the data subject via email, because we have direct contact with them, or via the subscription forms provided by the EPO to newsletters or any event. In accordance with the principle of data minimisation of the EPO DPR, PD Communication collects the minimum and necessary personal data so that the data subject can attend and participate in all the activities offered during meetings/events. Nevertheless, in the case of meetings/events with speakers, panelists or moderators, additional data may be collected to ensure smooth coordination and to support promotion. To promote meetings/events, the delegated controller usually publishes the agenda that may contain personal data of the speakers.

When meetings/events include minutes taking, the names of the participants and their function may be present in the minutes of the meeting, together with the participants' position organisation/institution and country. Depending on the topic and level of importance of the meeting/event, the minutes may be made available to the rest of the attendees.

During meetings/evens and in order to promote them through the EPO internal and external channels, as well as through multipliers, PD Communication usually captures screenshots, photographs and videos. Participants are informed in advance of it and are refrained to interact if they do not wish to appear in the multimedia content. The raw material collected is stored on the PD Communication internal database and deleted according to the EPO Retention Policy. Multimedia content published on the EPO social media channels is not removed unless it is decided that the content needs to be removed or a data subjects request to do so and because of legitimate grounds.

After the organisation of some meetings/events, PD Communication send by email or provides the attendees in the chat of the platform with a link to a User Satisfaction Survey. Their feedback is collected anonymously through MS Teams or Zoom forms and is kept according to the EPO Retetion Pollicy.

Additionally, contact details of certain categories of data subjects, such as those working for the main stakeholders with whom the EPO collaborates, such as institutions and national IP offices, may also be part of the EPO stakeholder database, which is a list that the delegated controller manages, and the EPO uses to send invitations to relevant meetings/events or season's greetings. The EPO stakeholder database has its own data protection statement that can be found on the epo.org.

Apart from the above, personal data may be processed by the delegated controller, the IT department of the EPO and even external

Purpose of Processing Transparency, Promotion, Organising and managing meetings/conferences/events/competitions, Communication, Accountability, Education, IP awareness, Coordinating any required follow-up activities

providers supporting the delegated controller to coordinating technical support needed before, during or after the meeting/event and to address access issues.

Finally, the EPO may use cookies on the meeting/event landing pages to offer you the best possible user experience. Information collected via the cookies installed might store and share your personal data with third parties, and according to the specific policies of the meeting/event platform used.

The processing is not intended to be used for any automated decision-making, including profiling.

Personal data will not be transferred to recipients outside the EPO that are not covered by Article 8(1) and (5) DPR unless an adequate level of protection is ensured. In the absence of an adequate level of protection, a transfer can only take place if appropriate safeguards have been put in place and enforceable data subject rights and effective legal remedies for data subjects are available, or if derogations for specific situations as per Article 10 DPR apply.

Data Retention Personal data processed by the EPO or the service providers under its supervision are stored for the period of time necessary to achieve the purpose for which they have been processed.

Personal data will be kept only by the EPO for the time needed to achieve the purposes for which it is processed and then deleted from its databases as follows:
A) For personal data related to sound, video and audio-visual recording/photographs of meetings/events, they are stored for educational, institutional, historical, informational and/or promotional purposes for a period ranging from 2, 10 or 25 years according to the retention categories reflected in the PD Communication Audio-visual Retention Policy, which can be provided upon request.
Meetings/events that can fall in the aforementioned retention categories are:
- Recurrent meetings/events with a low level of newsworthiness (2 years renewable);
- Non-recurrent meetings/events related to the core business of the EPO, for example related to the promotion of patent knowledge activities (10 years renewable);
- Recurrent meetings/events with a high level of newsworthiness related to the core activity of PD Communication at the EPO (e.g.: European Inventor Award, European Patent Convention 50 years celebration) (25 years renewable).

Data subjects and categories of personal data

Employees

Social	
Social Media Account	
Sensory and Electronic Information	
Visual Information	
Building area and site	
Building area and site	

Representation in EPO's Patent Granting Process	
Affiliation to Association of professional representatives	
Telephony Interaction Data	
Recorded Audio File	
Travel & Expense	
Expense Details	Travel Booking Details
Employment Information	
Active/Inactive Indicator	Business Unit Division
Contract Type	Department name and/or number
Job Title Role	Office Location
Personal Identification	
Age	First Name
Full Name	Gender
Surname	Nationality
Picture	
Education & Skills	
Educational Degrees	Languages
Project management experience	Technical expertise
General	
Any other information	Multimedia material
Contact Information	
Contact Details	Country
Working email address	
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Feedback received
Personal information provided voluntarily	
Browsing Information	

IP Address	

Contractors

General	
Any other information	Any other information that complies with the terms and conditions of the service
Contact Information	
Contact Details	Country
Emergency Contact Details	Mobile Phone Number
Personal Email	
Building area and site	
Building area and site	
Professional Experience & Affiliations	
CV	
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Employment Information	
Job Title Role	Language preference (of communication)
Browsing Information	
Browser type	Browsing Time
Cookie Information	IP Address
Education & Skills	
Languages	

Externals

Social	
Social Media Account	Social Media Contact
Phone Call Information	
Called Phone Number	Caller's Phone Number
Phone Call Date and/or Time	Phone Call Duration

Phone Call Interaction History	Phone Calling History
Ticketing	
Ticket related data	
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Employment Information	
Company Entity	Corporate Credit or Debit Card Numbers
Job Title Role	Previous Work History
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name
Gender	Surname
Nationality	Picture
Signature	
Education & Skills	
Education and Training History	Educational Degrees
Languages	
Matter/Log file	
Attachments	Metadata
General	
Answers to surveys, assessments or quizzes	Any other information
Attendees' lists	Legal opinions and assessments
Multimedia material	
Network/application Interaction Data	
Session content	Session details

Session metadata	
Health Data	
Dietary requirements	Health Data
Mobility needs	
Contact Information	
Contact Details	Home Address
Mobile Phone Number	Personal Email
Private Phone Number	Working email address
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Learning external events
Social learning inputs	
European Patent Register Data	
Data provided by the data subjects	
Professional Experience & Affiliations	
Affiliation	CV
Entry or deletion date as member of an association	Political Affiliation and Activities
Professional Memberships	Qualifications Certifications
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Feedback received	Personal information provided voluntarily
Financial	
Information for billing purposes (date, article, quantity)	
Family Information	
Child's nationality	Spouses's nationality
Browsing Information	
Browsing Time	Cookie Information
IP Address	Network Interaction History
System Logs	

System-, Application-, Security-related Server Logs	Web Servers Logs
Government Identifiers	
ID/Passport picture	

Former Employees

Contact Information	
Contact Details	Country
Mobile Phone Number	Personal Email
Professional Experience & Affiliations	
Affiliation	Professional Memberships
Trade Union Membership	
Representation in EPO's Patent Granting Process	
Affiliation to Association of professional representatives	
Financial	
Information for billing purposes (date, article, quantity)	
Employment Information	
Language preference (of communication)	
Personal Identification	
Full Name	Nationality
Education & Skills	
Languages	

Recipient of the personal data

Recipients of the data -The EPO Staff members from PD Communication and/or other departments or organisation units (e.g.: DG1, DG4 – Talent Academy, DG5 – Legal Affairs) involved in managing the initiative, project or activity.
-BiT Security, responsible for the maintenance of some of the databases used in the process of the organisation of events.
-Hospitality, security and logistics internal teams and external providers responsible for event logistic support, creation of audio-visual material or similar services in some of the meetings and events or provision of registration tools, event platforms or landing pages for events.
-Subcontractors, providers and suppliers of the relevant external providers that the EPO might establish a contractual relationship with.

Purpose of sharing For EPO Staff and external contractors personal data is shared to:
-Create reports/statisticts;
-Contact people for rehearsals;
-Send information about a training;
-Preparing badges for on-site event, name plates;
-Creating audiovisual materials (logistic teams);
For BiT: Maintenance and support purposes.
For hospitality, security and logistics and external providers:
-Checking list of participants to allow entry in EPO premises;
-Sharing list of dietary and health requirements for on-site hospitality.

Transfer

Transfer Yes

Country where data might be transferred - Processor (Vendors) Zoom - United States, Slido - United States, Huddle - United Kingdom, Microsoft - United States, SAP - Germany

Transfer to public authority and/or International Organisation

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Transfer mechanism(s)

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 474

Name European Inventor Award (EIA) and Young Inventors Prize (YIP)

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 47 - Procurement and Vendor Management, DG1 - 1 - Patent Granting Process, DG4 - 45 - CTO / BIT, DG4 - 41 - Finance

Entity Name - Controller (Entities) DG0 - 02 - Communication

External processors

Azavista

External processors	
Name Azavista	

Huddle

External processors	
Name Huddle	

Microsoft

External processors	
Name Microsoft	

Razuna

External processors

Name
Razuna

Poppulo

External processors
Name
Poppulo

Razuna

External processors
Name
Razuna

Amazon Web Services (AWS)

External processors
Name
Amazon Web Services (AWS)

Huddle

External processors
Name
Huddle

Amazon Web Services (AWS)

External processors
Name
Amazon Web Services (AWS)

Microsoft

External processors
Name
Microsoft

Award Force

External processors
Name
Award Force

Vok Dams

External processors	
Name Vok Dams	

1000heads

External processors	
Name 1000heads	

Description of the processing

Description In the context of both events the European Inventor Award (hereinafter “the Award”) and the Young Inventors Prize (hereinafter “the Prize”), personal data are processed by the EPO in the following situations:
Nominating the inventors and the finalists.
Personal data are collected when the applicant completes the online nomination form provided on the EPO website.
Inventors’ personal data are shared internally within the EPO and a pre-selection is made.
The processing is also necessary for deciding on the composition of the jury. Personal data of the selected inventors are then shared with the jury.
The EPO processed personal data about the jury members for their appointment as well as for the organisation of the meetings in which the jury members will select the finalists and winners. The rest of the selection process is performed by the jury. The jury decides who the finalists are.
For the Young Inventors Prize, the EPO will handle with the utmost care any children's personal data processed, such as pictures, video recordings or related information used for the evaluation of their applications and their possible participation in the event as a finalist. The EPO ensures that all necessary steps are taken to protect children’s interests, rights and freedoms when processing their personal data.

Selecting the finalists and winners
The jury deliberation meetings are carried out through MS Teams. In order to ensure that the selection procedure is accurate, as well as for minute-taking purposes, the meeting is recorded. Excerpts of the recording, as well as quotes from the participants might be published on the EPO website to create visual content for the promotion of jury’s participation in the event.

Holding the ceremony
EPO collects personal data directed from the nominees and process them to organise the ceremony. Personal data might be shared with the external providers entrusted with the organisation of the ceremony, travels and accommodations. After the ceremony, only the necessary data is kept in the EPO databases.
Public in general can attend the ceremony by streaming and personal data may be collected through the streaming platform for statistical purposes.
During the event, data subjects may have the possibility to actively participate in diverse ways. For example, by being part of the videos that the EPO may create for the ceremony together with the videos of the finalists or by interacting with the emojis provided in the landing page of the event or through the different social media where the EPO is present. Personal data about the online interactions may be collected for statistical purposes.

Purpose of Processing Maintenance and operational support, Organisation of meetings and the ceremonies, Creation of EPO staff engagement, Nomination and selection of the nominees, finalists and winners, Promotion of the competitions and the ceremonies, Creation of the promotional material

When the ceremony is held in presence, personal data processing may also be necessary for logistics support before (e.g. for managing the registration, accommodation and the provisioning of meals) during and after the ceremony. In such cases, the processing may include health related data.
Promoting the European Inventor Award and the Young Inventors Prize and their ceremonies.
The EPO promotes the Award and the Prize externally, and each year the EPO develops new ways of interacting with the public according to the trends on social media platforms and the technology.
Personal data are processed for sending information about upcoming Award, such as event invitations and reminders, the EPO shares your email address with an external provider that supports us with the mailing lists. If you are receiving these emails, it is because your personal data are part of a database shared internally among EPO departments in order to inform data subjects about future meetings or events.
We obtained the personal data from your registration at past events or from other sources (publicly accessible sources, another participant in a meeting/event entitled to provide data on your behalf, etc.). Data subjects are given the possibility to opt-out.
For the promotion of the Award and the Prize through different social media and press media communication channels, the EPO collects additional personal data from the finalists, jury members and other participants that may appear in the audio-visual material, and which is shared among different multipliers such as media agencies, influencers and European institutions. This audio-visual material is used not only to promote a specific edition of the Award or the Prize, but also the Award and the Prize as such and other EPO related Intellectual Property activities and events.
Personal data from EPO staff, jury members and stakeholders are also processed if they take part to the creation of the promotion material.
The EPO may organise voluntary activities among the EPO employees, so that both the Award and the staff engagement are promoted. For example, EPO employees could be enrolled in the production of a promotional video or be part of the audience at the ceremony.
Social media plugins and embedded YouTube videos are put in place not only on the web pages used to promote the event, such as the epo.org, the inventoraward.org, so that people can promote the event through their personal accounts.

Data Retention Once each edition ends, the external providers will delete any personal data processed from their files after having returned them to the EPO in accordance with the data protection agreements they have signed with the EPO.
Personal data about the inventors who are nominated one year may be also selected as a finalist in another year. To identify and encourage people to continue nominating candidates each year, and to be able to evaluate the development of an invention or an inventor's career, personal data of the person nominating, and the nominee provided in the nomination form are kept for a maximum of five years.
The personal data associated with the organisation of the Jury meeting will be erased the latest after 6 months following the last action in relation to the event. Nevertheless, in accordance with the data protection statement of the organisation of the jury meeting, some personal data needed for the promotion of the event might be kept for a longer period of time.
When you vote for the Popular Prize, all your personal data are directly anonymised, except for the name of the inventor you voted for. The anonymised data are only used for statistical purposes. The external provider will delete the collected data from their database two weeks after the close of the voting procedure, which is on the day of the event. However, please bear in mind that cookies might be kept on your device for a longer period.
The personal data associated with the organisation of the ceremony and its promotion in the form of staff and user engagement activities must be erased within two years of the last action related to the event. Nevertheless, some personal data may be kept for up to 25 years for educational, institutional, historical, informational and/or (internal and external) promotional purposes. Personal data published on the EPO's internal and external channels, such as EPOtv and the EPO website, or made available via other social media channels used by the EPO, such as YouTube, LinkedIn, Instagram and Facebook, will be limited as much as possible, for example by storing only the names, surnames and photos/videos of finalists and other participants in the ceremony.
If as a finalist agrees to be contacted for other activities relating to the EPO and join any future alumni network, the EPO will retain details such as biographical data and email address for as long as you agree to be part of that network.
If data subjects have subscribed to any EPO newsletter, the privacy statement for the EPO's newsletters and related alerts applies.
In the event of a formal appeal/litigation, all data held at the time the formal appeal/litigation was initiated will be retained until the proceedings have been closed.

Data subjects and categories of personal data

Externals

Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Employment Information	
Company Entity	Language preference (of communication)
Office Location	
Personal Identification	
Age	Date of Birth

Digital signature	Disability or Specific Condition
Gender	Signature
Education & Skills	
Educational Degrees	Languages
Project management experience	Technical expertise
General	
Multimedia material	
Network/application Interaction Data	
Session content	Session metadata
Health Data	
Dietary requirements	Health Data
Contact Information	
Emergency Contact Details	Home Address
Mobile Phone Number	Working email address
European Patent Register Data	
Data provided by the data subjects	
Professional Experience & Affiliations	
CV	Professional Memberships
Device Management Data	
Account ID	
Correspondence	
Personal information provided voluntarily	
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of a patent (claims, description, drawings, abstract)
Personal data potentially included within the content of patent procedure related information and publications	
Financial	
Bank Account Information	
Browsing Information	

Browsing Date and Time	Cookie Information
IP Address	Number of requests from the (hashed) IP address per period
Government Identifiers	
ID/Passport picture	Passport Number

Contractors

General	
Answers to surveys, assessments or quizzes	Any other information
Assessment and legal opinions	Multimedia material
Votes	
Social	
Social Media Account	
Health Data	
Dietary requirements	Mobility needs
Professional Experience & Affiliations	
CV	
Correspondence	
Any other information	
Travel & Expense	
Expense Details	Travel Booking Details
Employment Information	
Assessment and legal opinions	Company Entity
Department name and/or number	Job Title Role
Language preference (of communication)	Line Reporting Manager
Personal Identification	
First Name	Full Name
Gender	Surname
Nationality	Picture
Education & Skills	

Languages	
User Account Information	
Account Number	Application Specific User Role
Membership Permissions	Ownership Permissions
Third-party User Identifier	User ID

Employees

Contact Information	
Contact Details	Country
Mobile Phone Number	Teleworking address
Working email address	
Building area and site	
Building area and site	
Correspondence	
Additional Information which might be provided in the course of exchanges	Chat content
Personal information provided voluntarily	
Employment Information	
Job Group	Job Title Role
Language preference (of communication)	Line Reporting Manager
Office Location	
Browsing Information	
Cookie Information	IP Address
Personal Identification	
Full Name	Gender
Nationality	Picture
Education & Skills	
Languages	Project management experience

Recipient of the personal data

Recipients of the data The organiser team composed by EPO staff and external contractors have access to the data. In addition, some colleagues from Principal Directorate Communication and other departments such as DG1 have also access, so that they can support the EIA team on the analysis of the nominated patent or the promotion of the ceremony.
Personal data may be disclosed to third-party service providers for the purpose of organising the event, creating and promoting the campaign, maintaining and supporting the platforms created for the nominations, the event and the Popular Prize, and ensuring compliance with security and health-related standards. Additionally, the audiovisual material produced may be shared with other entities for promotional purposes, and with the public in general through the EPO social media accounts and website.
In general, promotional material is shared with the public via several communication channels.

Purpose of sharing

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) Contractual clauses (e.g. DPA), The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors)
Huddle - United Kingdom, Razuna - United States, Microsoft - United States, Amazon Web Services (AWS) - United Kingdom

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, Sub-processor(s) storing the personal data, Service provider processing data for the creation of anonymous statistics

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".

Contact Details

Data controller: European Patent Office

Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany

Contact details: DPOexternalusers@epo.org

Data Protection Officer Name: Simona Barbieri

Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 496

Name EPO's email newsletters, alerts and subscription centre

Delegated Controller and processor within the EPO

Entity Name - Processor (Entities) DG4 - 46 - CIO / BIT, DG5 - 51 - European and International Affairs, DG5 - 54 - Patent Intelligence

Entity Name - Controller (Entities) DG0 - 02 - Communication

External processors

Poppulo

External processors	
Name Poppulo	

Description of the processing

Description This data protection statement applies only to the data we collect via the EPO website related to subscriptions to the following EPO email newsletters and alerts:

- EPO newsletter
- Official Journal alerts
- European Inventor Award and Young Inventors Prize newsletter –
- User consultation alerts
- Online services event alerts
- Events e-alerts

We collect contact information, preferences and selections, information about how users access our emails and information about newsletter usage.
The information we hold on individual users will depend on what email publications they have subscribed to. We do not collect all categories of data for all users.
To collect the data for anonymised statistics and send the email newsletters and alerts, the delegated controller uses Poppulo's Newsweaver tool. Some departments have also access to the tool, but they have an account that will allow them to only manage the newsletters or alerts of their interest.
Users can unsubscribe at any time by using the link provided in the footer of the newsletter. In this link they can also find more information about the subscription options and whether they want to stop receiving all EPO mailings or a specific mailing. If they encounter any problems, they can email website@epo.org with the words "Unsubscribe newsletter" in the subject line.
If users contact us with a question or problem relating to a subscription to one of our email publications, the delegated controller may access or edit their individual data in order to answer their query or adjust your preferences or subscriptions as requested. We will not do so in any other circumstances.
Personal data processed by the data controller or the service providers under its supervision are generally stored for the period of time necessary to achieve the purpose for which they have been processed.
Contact details for the mailing lists and alerts as well as users' preferences are kept until the data subjects unsubscribe themselves from the mailing list.
Information provided by users in the course of an email exchange and which may contain personal data, because of a particular problem with the access to any newsletter, or because they provided their opinion or any other request with respects to the newsletters and alerts, will be stored by PD Communication only for the time necessary to solve the issue or give them an answer.
Users' personal data is always processed in accordance with the EPO retention policy, which can be provided upon request.

Purpose of Processing We also collect data on open rates for our email publications. We do this in order to identify the topics our readers find most interesting. These statistics enable the EPO to adapt and improve their services., Supporting users in managing and maintaining their subscriptions and preferences, Providing subscription services to users specific to their interests, Fixing any technical issues related to subscriptions., We collect and process personal data for the sole purpose of enabling us to perform tasks carried out on the basis of the European Patent Convention (EPC) and to fulfil our mission.

Data Retention Personal data processed by the data controller or the service providers under its supervision are generally stored for the period of time necessary to achieve the purpose for which they have been processed.

Contact details for the mailing lists and alerts as well as users' preferences are kept until the data subjects unsubscribe themselves from the mailing list.

Information provided by you in the course of an email exchange and which may contain personal data, because of a particular problem with the access to any newsletter, or because you provided your opinion or any other request with respects to the newsletters and alerts, will be stored by PD Communication only for the time necessary to solve the issue or give you an answer.

Your personal data is always processed in accordance with the EPO retention policy, which can be provided upon request.

In the event of a formal appeal/litigation, all data held at the time the formal appeal/litigation was initiated will be retained until the proceedings have been closed.

Data subjects and categories of personal data

Externals

General	
Any other information	Any other information that complies with the terms and conditions of the service
Contact Information	
Contact Details	Country
Personal Email	Working email address
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Personal information provided voluntarily	
Employment Information	
Language preference (of communication)	
Personal Identification	
First Name	Full Name
Surname	

Recipient of the personal data

Recipients of the data - Personal data are disclosed on a strict need-to-know basis to the EPO staff working in PD Communication and other business units managing the different newsletters and alerts. Access to the tool is restricted to a limited number of staff to ensure data security.
- Business Information Technology might have access to the data for technical support or/and IT service maintenance.
- Third-party contractor who provides the EPO with technical tools for email newsletter management.

Purpose of sharing - Management of the tool and sending newsletter and alerts according to users' preferences.
- Technical support and service maintenance

Transfer

Transfer No

Country where data might be transferred - Processor (Vendors)

Transfer to public authority and/or International Organisation

Reasons for the transfer

Transfer mechanism(s)

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

More information about this processing activity can be found in the related data protection statement available on the EPO data protection and privacy notice, under "Information on the processing of personal data in EPO products and services".