Data protection statement on the processing of personal data in the context of Contractor Management (creation, on/offboarding, deletion of EPO external contractors)

Protecting your privacy is of the utmost importance to the European Patent Office (EPO). We are committed to protecting your personal data and ensuring respect for data subjects' rights when performing our tasks and providing our services. All data of a personal nature that identify you directly or indirectly will be processed lawfully, fairly and with due care.

The processing operations described below are subject to the EPO Data Protection Rules (DPR).

The information in this statement is provided in accordance with Articles 16 and 17 DPR.

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 delegating another EPO staff member to act as EPO contract manager on their behalf; or by delegating an external contract manager, which demands prior approval by the EPO contract manager or by his/her delegate(s).

1. What is the nature and purpose of the processing operation?

This data protection statement relates to the processing of Contractor Management which entails the creation, on/offboarding, deletion of EPO external contractors from EPO systems.

Personal data are processed 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.

The processing is not intended to be used for any automated decision-making, including profiling.
The Contractor Management processing operation does not process personal data in the sense illustrated in Art.12 DPR; namely, no processing is done of data subject's criminal convictions, offences, suspicions regarding offences, or security measures taken against the data subject in the context of a criminal (or administrative) procedure.
In the event a contractor is prematurely offboarded, this is done in Contractor Management application without specifying any circumstantial justifications.

Your 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).

2. What personal data do we process?

The processing operation processes personal data of externals, of contractors and of EPO employees.
Personal data of externals are processed during the early phases of provisioning; after successful provisioning and onboarding, externals become contractors.
The following categories of personal data may be processed:

For externals:
- Contact information: work email address;
- Personal identification: first name, last name, gender, data of birth, nationality, signature;
- Employment information: Company entity, contract type, department name/number, office location, working patterns, preferred language of communication.

For contractors:
- Contact information: work email address;
- Personal identification: first name, last name, gender, data of birth, nationality, signature;
- Employment information: Company entity, contract type, personnel number, line reporting manager, start date, end date, department name/number, office location, working patterns, preferred language of communication;
- EPO site;
- User account information: UserID, application-specific user role, third-party user identifier;
- Device Management Data such as account ID, Azure Active Directory Device ID; EAS deviceID, Encryption Key, 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, AppleID for iOS/iPadOS devices;
- Physical and/or digital identifiable assets such as IMEI (International Mobile Equipment Identity) number, mobile device name, mobile device serial number, vendor model of workstation, workstation's serial number, workstation's hostname (physical or virtual).

For EPO employees:
- Contact information: work email address;
- Personal identification; first name, last name;
- User account information: UserID, application-specific user role.

3. Who is responsible for processing the data?

Personal data are processed under the responsibility of Chief Information Officer/PD 4.6, acting as the EPO's delegated data controller.
The central team of administrators who register contractors are in UserReg team within BIT 4634 End-User Computing, or in the team registration.externals@epo.org .
Internal processors might belong to any EPO organisational unit; internal processors are given any of these four roles defined in Contract Management application: 1) EPO contract administrator; 2) vendor administrator; 3) additional EPO contract administrators; 4) additional vendor administrator.
External contractors involved in providing and maintaining the underlying platforms and services may also process personal data, which can include accessing it.

4. Who has access to your personal data and to whom are they disclosed?

Personal data are disclosed on a need-to-know basis to:

- the EPO staff working as EPO contract administrator, vendor administrator, additional EPO contract administrator or additional vendor administrator.

- The central team of administrators who receive and approve 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 as extensions, re-hire, (premature) offboarding, etc. Unlike in case of onboarding requests, none of the resulting updates require the involvement of the central administrator team.

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.

5. How do we protect and safeguard your personal data?

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.

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).

6. How can you access, rectify and receive your data, request that your data be erased, or restrict/object to processing? Can your rights be restricted?

You have the right to access, rectify and receive your personal data, not to be subject to a decision based solely on automated processing, to have your data erased and to restrict and/or object to the processing of your data (Articles 18 to 24 DPR).

If you would like to exercise any of these rights, please write to the delegated data controller at DP_BIT@epo.org . In order to enable us to respond more promptly and precisely, you always need to provide

certain preliminary information with your request. We therefore encourage you to fill in this form (for externals), this form (for internals) and submit it with your request.

We will reply to your request without undue delay and in any event within one month of receipt of the request. However, Article 15(2) DPR provides that this period may be extended by two further months where necessary in view of the complexity and number of requests received. We will inform you of any such delay.

7. What is the legal basis for processing your data?

Personal data are processed on the basis of:

- article 5(a) 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 Office's management and functioning*").

8. How long do we keep your data?

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.

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.

9. Contact information

If you have any questions about the processing of your personal data, please write to the Delegated Controller at DP_BIT@epo.org or to the Data Protection Office at DPOexternalusers@epo.org .

Review and legal redress
If you consider that the processing infringes your rights as a data subject, you have the right to request review by the controller under Article 49 DPR and, if you disagree with the outcome of the review, the right to seek legal redress under Article 50 DPR.