Europäisches Patentamt
European Patent Office
Office européen des brevets

50 years 1973 / 2023 EUROPEAN PATENT CONVENTION

Data Protection Report 2022

Annex to the Annual Review

epo.org

Executive summary

The innovative framework for the protection of privacy and personal data at the EPO, which was adopted by the Administrative Council in June 2021, entered into force on 1 January 2022. The first year of the implementation of the new framework was a success for the Office and the Data Protection Office (DPO).

The mapping of the processing operations of the EPO involving personal data was completed, with only a few exceptions, by the network of Data Protection Liaisons during the transition period which ended by July 2022.

The DPO created the essential instruments for the detection and management of privacy and data protection risks. These included the Privacy and IT Security Risk Assessment and the Data Protection Impact Assessment.

In relation to the transferring of personal data, a series of instruments was created. These included the Adequacy Referential, providing guidance for assessing whether the protection afforded by a third country or international organisation can be considered equivalent to that offered by the EPO; a Transfer Impact Assessment model; and guidance on transfers to international organisations and non-EPC public authorities, providing interpretations of the application of Articles 9 and 10 of the Data Protection Rules (DPR).

In the context of risk management and mitigation, a comprehensive data protection compliance framework was adopted, including mechanisms for regular Data Protection Self-Assessments by the delegated controllers, Data Protection Audits and Data Protection Inspections.

The DPO continued its awareness-raising activity. We published a series of guidance documents to enhance the understanding of the new framework and fully integrate the DPR into the processes of the Office. As part of the efforts towards higher data protection awareness, the DPO created an e-learning on data breaches and two non-mandatory e-learnings on data subjects rights and the accountability principle in data protection. These are in addition to the two e-learning modules that were made mandatory for all staff in 2021.

With the implementation of the new legal framework well on its way, the Office is equipped to face the challenges of protecting privacy and personal data in the digital world. We can also reassure staff, partners and users that their data are safe and secure in the EPO environment. Finally, the EPO is ready to share its experiences and best practices in the field of these fundamental rights with European public administration entities.

Contents

1. Introduction

With the adoption of the Data Protection Rules (DPR) and the changes to the Service Regulations for European Patent Office (EPO) employees by the Administrative Council in June 2021, the EPO reached the first milestone in the transformation of its data protection framework, which continues to have a visible impact on all areas of its activities.

In accordance with the fundamental principles of the DPO Strategy and Planning 2021-2023, "Anticipation-action-unity", the DPO pursued a strategy based on five pillars.

Figure 1: DPO strategy

Source: DPO

The highlights of the DPO's activities in 2022 were:

- the set-up of the publicly available all-in-one Register of processing operations and the publication of data protection statements, which ensure transparency by explaining to all data subjects why and how their personal data are processed by the EPO
- a wide-ranging data protection risk management framework, including instruments for detecting and managing privacy and data protection risks, such as privacy and IT security risk assessment (PSRA), and data protection impact assessment (DPIA)
- the adoption of a comprehensive data protection compliance framework, including mechanisms for regular data protection self-assessments by the delegated controllers, data protection audits and data protection inspections
- the creation of a series of instruments to enable and facilitate the transfer of personal data, such as the adequacy referential (which provides guidance on assessing whether the protection afforded by a third country or international organisation (IO) can be considered equivalent to that offered by the EPO), a transfer impact assessment (TIA) mechanism, and a

guidance on transfers to IOs and non-EPC public authorities, which provides interpretations of the application of Articles 9 and 10 DPR

- extensive awareness-raising measures, including numerous guidance documents and explanatory notes, the launch of a Data Protection Wiki (guidance and explanation on the Articles of the DPR published online internally by the DPO) and a number of training courses and new e-learning modules

All this was accompanied by a record number of internal consultations (over 600), carried out by the DPO, on a vast range of data protection issues touching upon all areas of the EPO's activities.

In addition, the DPO continued to seek synergies and co-operate with other international organisations and public institutions, with a view to contributing to the harmonisation of practices and raising awareness of the importance of data protection.

This annual report, which under Article 43 DPR is submitted annually by the DPO to the Administrative Council, the President of the Office and the President of the Boards of Appeal, highlights the Data Protection Officer' s activities in 2022, focusing on the results achieved in line with the DPO Strategy and Planning 2021-2023 and on upcoming activities, deliverables and challenges.

2. Data Protection Office

The Data Protection Office (DPO) is the focal co-ordination point for all activities included in the DPO Strategy and Planning 2021-2023. The DPO fulfils its mandate and responsibilities by ensuring that the EPO respects the fundamental rights to privacy and data protection. The DPO is supported in this by the network of data protection liaisons (DPLs).

The President of the Office appoints the Data Protection Officer and their deputy for a term of three to five years, based on their professional qualifications (particularly their expert knowledge of data protection law and practices) and their ability to fulfil the duties provided for in the DPR. Their duties are governed by Articles 41 to 43 DPR.

The Data Protection Office is the focal co-ordination point for all activities included in the DPO Strategy and Planning 2021-2023

In addition to their other duties, the DPO responds to requests from the Data Protection Board (DPB) within the sphere of its competence, while co-operating and consulting with the DPB at the latter's request or at its own initiative. The DPO facilitates co-operation between the DPB and the EPO, particularly with regard to data protection audits and inspections, complaint handling, data protection impact assessments and prior consultations.

2.1 Data Protection Liaisons network

The Data Protection Liaisons (DPLs), who are organised in a network and work closely with the DPO, are key players in the implementation of the privacy and data protection principles and requirements laid down in the DPR. The DPLs assist delegated controllers in complying with their obligations under the DPR.

Throughout 2022, the DPO chaired regular meetings of the DPL network to ensure the coherent interpretation and implementation of the DPR at the EPO. The network spreads knowledge and makes sure that useful practical experiences are shared. The DPLs also acquire knowledge that they can subsequently pass on to their respective departments or units.

DPLs play a crucial role in implementing the principles and requirements of data protection laid down in the DPR

Throughout the year, the DPO-DPL meetings focused on mapping out and documenting processing activities and DPL training, supported by the provision of data protection documentation by the DPO (e.g. handling of data subjects' requests and data breaches) and dedicated training sessions on the use of selected risk management package components.

In addition, the DPO continued to populate the data protection knowledge database for the DPLs. In addition to the guidance documents issued by the DPO, this database contains further opinions and guidance released by European and national data protection authorities, academic articles on relevant topics and templates as a source of knowledge for the DPLs. It provides them with a wider perspective on the interpretation of data protection concepts and make their tasks easier. The DPO updates and extends this database constantly to ensure that it covers the latest developments in privacy and data protection.

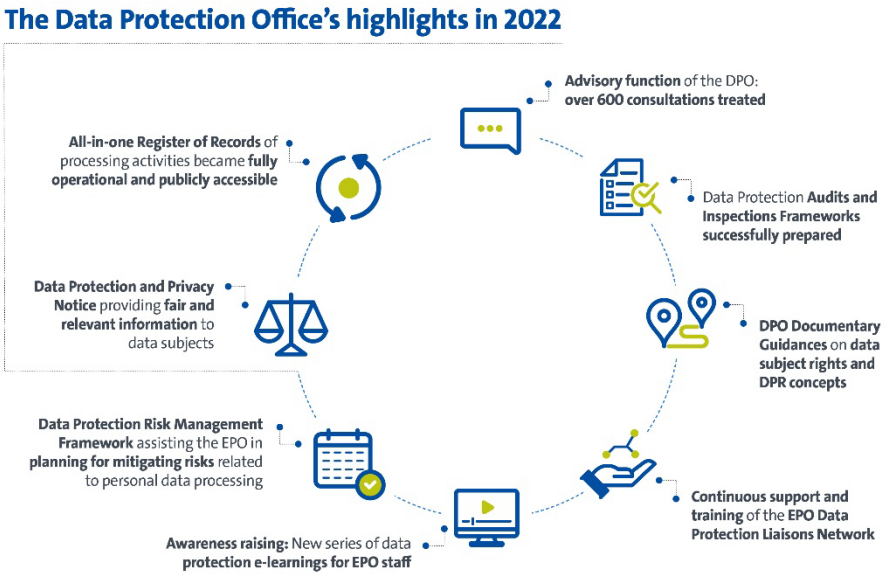
3. Main objectives in 2022

The EPO's Strategic Plan 2020-2023 (SP2023) set out the initiatives that would lead to the creation and implementation of an improved data protection policy at the EPO.

In the context of the DPO Strategy and Planning 2021-2023, the objectives for 2022 included:

- creation of the risk management instruments and templates
- creation of the frameworks for data protection audits and inspections
- continuing to raise awareness in an adequate manner and provide training and communication to accompany the introduction of the new rules
- maintaining and enhancing co-operation with other international organisations and public institutions and the exchange of best practices to ensure that the EPO remains abreast of technological innovations and transformations in the area of privacy and data protection

Figure 2: The Data Protection Office's highlights in 2022



Source: DPO

4. Data protection: legal framework and policies

4.1 Applicability of data protection principles throughout the organisation

The DPR apply to the EPO's processing of personal data. However, they do not apply to the Administrative Council and further ad-hoc committees within the EPO.

Creating legal frameworks to cover all types of processing of personal data across the Organisation

To ensure consistency within the European Patent Organisation in the processing of personal data, applying the same principles and enabling a smooth running of processing operations in which both the Council and the Office are involved, while guaranteeing that the highest standards of protection of the data subjects' rights apply at all times and achieve full implementation of the obligations enshrined in the DPR, the DPO joined forces with the Administrative Council Secretariat and the legal services of the Office to prepare a data protection framework applicable to the other organ of the European Patent Organisation, the Administrative Council, and further bodies and committees not covered by the EPO DPR.

The creation of such a framework and the application of the principles and mechanisms enshrined in the DPR to the processing of personal data by the Administrative Council and other bodies and committees is part of the DPO's continuous efforts to apply the data protection principles across all of the activities of the European Patent Organisation.

4.2 Decision of the President of the EPO identifying the delegated controllers

The list of delegated controllers is updated regularly to reflect organisational changes

Under Article 28 DPR, the President of the EPO acts as the controller of the personal data processed by it, unless specified otherwise. As such, the controller has the power to delegate the authority to determine the purposes and means of processing certain personal data to an operational unit, represented by its head ("delegated controller"). In accordance with the principles of transparency and accountability, it is essential that the delegated controllers are properly identified within the organisation and in the data protection documentation made available to the data subjects.

The DPO prepares regularly for the President, at least once a year or more often if needed, updates of such decisions to reflect the organisational changes which have occurred in the meanwhile.

Therefore, also in 2022, following organisational changes, the President of the EPO adopted a decision in 2022 to update the list of delegated controllers representing the operational units to which the authority to determine the purposes and means of processing certain personal data had been delegated, in line with Article 28(3) DPR.

4.3 Decision of the President of the Boards of Appeal appointing a delegated controller

Under Article 28(2) DPR, the President of the Boards of Appeal (BoA) acts as the controller with respect to the personal data processing operations carried out as part of the judicial activity of the BoA and in exercising functions and powers under the Act of Delegation.

In 2022, the President of the BoA appointed his deputy as delegated controller with respect to the personal data processing operations carried out in exercising administrative functions and powers under the act of delegation. This delegation does not concern the personal data processing operations carried out as part of the judicial activity of the BoA.

4.4 Cookie policy

In line with current requirements and best practices across the EU, the DPO drafted a cookie policy in 2022 concerning the cookies used on the EPO's current websites (i.e. epo.org, new.epo.org and the EPO Bulk Data Distribution Service). The policy is published in the data protection and privacy notice on the EPO website.

4.5 Video surveillance policy

In 2022, the DPO supported the creation of a new EPO video surveillance policy (Circular 421) to provide the framework and guiding principles according to which the EPO's video surveillance system (VSS) is designed, deployed and used. The Circular describes the VSS and the safeguards put in place by the EPO to ensure the protection of the personal data, privacy and other fundamental rights and

legitimate interests of individuals affected by the VSS. The Circular will be updated in the future to ensure that the VSS is in continuous compliance with the legal framework for the protection of personal data at the EPO and related rules.

5. Data protection: complementary instruments and procedures

For data protection to become integral to the activities of the EPO, the adoption of ancillary instruments and mechanisms is essential. It will:

- guarantee transparency, demonstrate compliance and ensure accountability
- mitigate privacy and data protection risks, enhancing the trust of staff and public in the EPO's data processing activities
- enable individuals to control their personal data and to exercise and enforce their rights effectively
- successfully implement the digital transformation, taking privacy requirements and specific business goals into account from the start
- guarantee further alignment and harmonisation with best rules and practices at the international level

In 2022, the EPO adopted the specific instruments, mechanisms, frameworks and procedures described below to complement the DPR and regulate the implementation of the new framework.

5.1 Data protection statements and privacy notice on the EPO website

The completion of the data protection documentation and its availability online – both on the intranet and the EPO's website - have contributed to strengthening data subjects' rights by making information readily available and describing the mechanisms for exercising these rights in a clear and accessible way.

Throughout 2022, the DPO regularly updated the content of the data protection and privacy notice published on the EPO website to ensure that it continued to provide external data subjects (users and stakeholders) with all key information on the special features of how the EPO processes personal data and its adherence to the principles of compliance and accountability.

In particular, the notice explains the purpose of processing operations, how the EPO processes data and the safeguards in place. It also informs data subjects of their rights and describes how to exercise them. The data protection policy is also updated regularly with new or amended data protection statements, published by the relevant delegated controllers, as well as relevant pieces of legislation, i.e. circulars or decisions of the President of the EPO and/or President of the Boards of Appeal.

5.2 Implementation of Circular 420

In 2021, the President of the EPO adopted Circular 420 implementing Article 25 DPR. This Circular provides guidance for all stakeholders concerned by

describing the concept of restrictions, clarifying the differences between two types of limitations that can be applied to the rights of the data subjects and the criteria for applying restrictions. In addition, it outlines safeguards for data subjects that are needed to prevent unlawful access, transmission or transfer of personal data when applying restrictions.

Before applying a restriction, the delegated controller must conduct a necessity and proportionality test on a case-by-case basis. In 2022, the DPO supported the units of the EPO in creating clear mechanisms and documentation for the necessity and proportionality test to be conducted when applying a restriction, thus ensuring full application of the accountability principle.

5.3 Explanatory memorandum on processing personal data in appeal proceedings before the Boards of Appeal

Following the decision of the President concerning the processing of personal data in patent grant and related proceedings, as published in the EPO's Official Journal in 2021, the DPO supported the President of the Boards of Appeal to prepare a decision on the processing of personal data in appeal proceedings before the BoA. These decisions align the interpretation of the DPR with the EPC and were written in response to queries from users and other stakeholders, as well as to meet their expectations.

5.4 Explanatory note on the transmission and transfer of personal data by the EPO

The EPO continuously needs to transmit and/or transfer personal data to recipients, such as public authorities within the territory of the EPC’s contracting states, national intellectual property offices, private entities (processors) within or outside the European Economic Area (EEA), public entities in third countries and international organisations.

In everyday practice, this sharing of personal data (through disclosure, dissemination or otherwise), as well as the provision of access to them, may be necessary for different reasons. Examples include international co-operation activities, dealings with foreign public authorities, outsourcing of services to external providers located within or outside the EEA or the use of transnational services when providing certain arrangements to staff.

Under the DPR, specific conditions are set forth for the transmission and transfer of personal data by the EPO. To help the EPO’s delegated controllers legitimise data transfers, the DPO issued an explanatory note on the transmission and transfer of personal data, together with an analysis of transfers to international organisations and non-EPC public authorities.

The document aims to give a brief outline of the DPR concepts of transmission and transfer and the respective requirements met by the EPO (the data exporter), along with the various types of recipients (data importers). Furthermore, it elaborates on how the relevant provisions of the DPR provide guidance for a thorough analysis and assessment of circumstances, specificities and risks by embedding a risk-based approach. It also provides various instructions, measures and safeguards to meet business needs effectively while preventing

and mitigating risks, and to ensure the free movement of personal data between the EPO and the various recipients based on criteria that include necessity, proportionality, adequacy of protection, transparency and accountability.

In 2022, an Adequacy Referential was issued to provide guidance to the President of the Office when assessing whether the protection afforded by a third country or international organisation can be considered essentially equivalent to that of the EPO from a data protection perspective. It establishes the key data protection principles and concepts that should be present in the legal framework of a third country or international organisation for an adequacy decision to be granted by the President of the Office, pursuant to Article 9(2) and (3) DPR.

To facilitate this assessment, the DPO prepared an adequacy referential checklist. For the purposes of Article 9(2) DPR, the President also adopted a decision concerning countries and entities that are considered as ensuring adequate protection of personal data. This decision includes a list of the countries (or territories or sectors within a country) and entities that are currently deemed to have a legal framework for data protection that is essentially equivalent to that of the EPO.

In addition, a transfer impact assessment (TIA) was issued to guide the delegated controllers in assessing the level of protection offered by the recipient, the risks a transfer may entail to the fundamental rights and freedoms of data subjects and, if applicable, the appropriate mitigation of such risks.

More details about the adequacy referential and TIA are provided in section 7 below. Both instruments are components of the risk management package.

5.5 Consent form template

Consent is one of the lawful basis for processing provided for under Article 5 DPR. The DPR sets a high standard for consent, which offers individuals real choice and control over the processing of their personal data. Where consent is the only and/or most appropriate lawful basis for processing, the controller must be able to demonstrate that the request for consent is presented in a clear and intelligible manner.

Consent must be freely given, specific, informed and unambiguous, and the data subject has the right to withdraw consent at any time. Where the use of consent is deemed appropriate, the possibility of its withdrawal should always be reflected by a data protection statement, disclaimer or form.

To support delegated controllers whenever consent is identified as the single and/or most suitable legal basis for processing personal data, the DPO prepared a model consent form that fulfils such requirements.

5.6 Further policies in preparation

In addition, the various departments of the Office, supported by the DPO, are drawing up the following policies, with a view finalising them in 2023:

- The social media handbook: the DPO has worked in close co-operation with Principal Directorate Communication to establish a policy on the use of social

media by the Office. In 2021, PD Communication launched a pilot project with a view to assessing the EPO's needs and exploring ways of using social media to support its activities to greater effect. The handbook was drafted in 2022 and is currently being finalised.

- Audio-visual retention policy: the DPO supported the EPO's Principal Directorate Communication in drafting an audio-visual retention policy, which will create greater transparency regarding the retention periods of audio-visual content. The policy aims to establish the retention criteria of multimedia content for EPO meetings, events and additional content published on different EPO channels.
- The Unified Patent Court (UPC): the DPO provided an analysis of the data protection elements to be taken into account, as well as the available options for legitimising the identified exchanges of personal data between the EPO and the UPC. In November 2022, the two institutions signed an agreement on the exchange of information, including a data protection clause in which they agreed to enter into a specific agreement on the processing of personal data.
- The DPO is to support the drafting of the data protection framework for the processing of personal data as part of the judicial activities of the BoA.
- The DPO is drafting explanatory guidelines on the concepts of anonymisation and pseudonymisation under the DPR.

6. Data protection: operational compliance

The entry into force of the DPR on 1 January 2022 was followed by a six-month transition period. This enabled the Office to bring data processing operations that were ongoing prior to the adoption of the new DPR into line with the new framework, e.g. with regard to fulfilling the obligation of documentary compliance.

Throughout 2022, the series of administrative instructions, guidelines and other operational documents issued by the DPO in 2021, which among other things comprised work instructions for delegated controllers and DPLs and a personal data breach manual, were amended regularly and additional documents were adopted to complete the data protection framework. This enabled the EPO to successfully implement the DPR and achieve documentary and implementary compliance.

6.1 Comprehensive mapping of processing operations and all-in-one Data Protection Register

The comprehensive mapping of the EPO's personal data processing operations constituted the first achievement in documentary compliance with regard to data protection and is key to ensuring transparency towards all data subjects. The results of the mapping provide the required content for the all-in-one EPO Data Protection Register, as defined under Article 32 DPR.

Following up on the work performed in 2021, the DPLs continued to provide assistance to the delegated controllers in the first half of 2022 to complete the data protection documentation and ensure transparency towards data subjects. This documentation comprises records of processing operations as part of the new central register and published data protection statements. It enables the

EPO to abide by the principles of transparency and accountability enshrined in the DPR by demonstrating compliance with the highest standards of personal data protection.

As from 2023, the DPO will regularly review a sample of personal data processing operations selected from the Register. This is part of a risk-based approach to assess the documentary compliance of the records of processing operations and their practical implementation, in line with the requirements laid down in the DPR.

A tool has been designed that facilitates implementation of the revised legal data protection framework under SP2023, with modules including data mapping, assessment automation, personal data breaches response and cookie compliance website scanning and consent.

The DPLs received continuous training from the DPO on using the tool to create records of processing activities of their respective operational units. The records are part of the Register, which is publicly accessible pursuant to Article 32(6) DPR (with the exception of confidential records). The records are published on the EPO intranet for all EPO staff. Records concerning personal data of external users are also available on the EPO website.

The Register is maintained by the DPO.

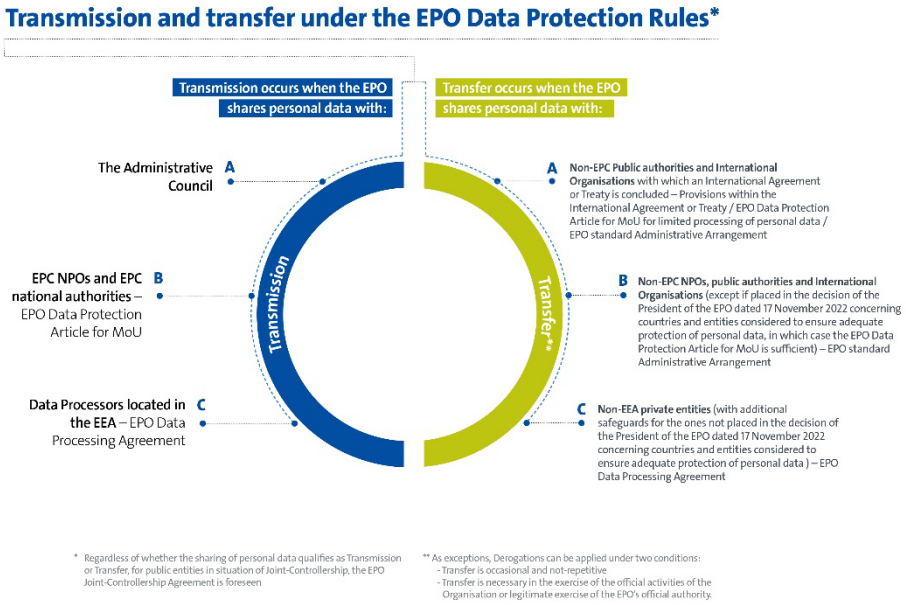
7. Data protection: risk management

In 2022, the DPO finalised the instruments in the risk management package to complement and enhance the EPO's risk management framework by integrating privacy and data protection. These instruments include the:

- **Privacy and IT security risk assessment (PSRA)** methodology and template, which supports the delegated controllers in evaluating risks to personal data associated with their business operations and provides guidance on the adoption of relevant security measures. It is mainly focused on electronic personal data processing by external providers and based on IT networks and systems, e.g. Software-as-a-Service ('SaaS').
- **Data protection impact assessment (DPIA)** methodology and model, which guides the delegated controllers on when and how to carry out this assessment (i.e. processing operations potentially resulting in "high risks" to the rights and freedoms of data subjects, as defined under Article 38 DPR) and helps them to identify and minimise data protection risks to ensure and demonstrate compliance with the DPR. The DPO analysed the Register, identified the processing operations that may be subject to the DPIA requirements and initiated this assessment with the relevant delegated controllers with a view to completing it in 2023.
- **Adequacy Referential**, which provides guidance to the President of the EPO when assessing whether the protection afforded by a third country or international organisation can be considered adequate from the data protection perspective. It establishes the key data protection principles and concepts that should be present in the legal framework of a third country or international organisation for an adequacy decision to be granted by the President. In this regard, the President adopted the decision dated 17 November 2022 concerning countries and entities that are considered as ensuring adequate protection of personal data, which complements the DPR.

- **Transfer impact assessment (TIA)**: under the DPR, transfers are permissible only if the recipient ensures a level of protection of the rights and freedoms of individuals that is comparable to that guaranteed by the DPR (Article 9 DPR). The methodology guides the delegated controllers in assessing the level of protection offered by the recipient, the risks the transfer may entail to the fundamental rights and freedoms of data subjects and, if applicable, the appropriate mitigation of such risks.
- **Analysis of transfers to IOs and non-EPC public authorities**, which complements the two instruments above and seeks to provide possible interpretations as to the scope of the application of Articles 9 (transfers) and 10 (derogations) DPR in the context of identified transfers from the EPO to the national patent offices of third countries or international organisations. The analysis builds and expands on the previously mentioned explanatory note issued by the DPO on the transmission and transfer of personal data by the EPO.
- **Data sharing instruments**, which provide appropriate guarantees for transmissions (Article 8 DPR) or transfers (Article 9 DPR) of personal data to public entities; because specific data protection provisions should be inserted into legally binding and enforceable instruments, such as bilateral or multilateral administrative arrangements or memoranda of understanding. The DPO has developed different instruments, namely two administrative arrangement models and a data protection clause for memoranda of understanding.
- **Joint controllership agreement**, pursuant to the requirements under Article 29 DPR, which aims to regulate the relationship between the EPO and one or more public entity controllers when these qualify as "joint controllers" - namely if they jointly determine the purposes and means of the processing of personal data as part of shared activities.
- Guidance on **data protection criteria for tender procedures**, which define recommendable data protection selection or award criteria for tender procedures involving the processing of personal data to reduce the risk of pre-selecting and eventually contracting external providers that have not implemented privacy and security measures in line with EPO standards.
- New **data processing agreement (DPA) template**, which is a binding contract that regulates the roles and responsibilities of the external providers together with the scope and purpose of the processing operations. The model reflects the principles and requirements of the DPR and should therefore, in principle, be signed with the new service or tool provider during the procurement procedure.
- **Data protection clauses assessment tool**, for exceptional cases where an external provider does not wish to sign the EPO DPA and instead submits its own, to provide preliminary guidance on the compatibility of the provider's DPA with the DPR requirements. The tool includes the relevant legal basis in the DPR and the GDPR (for information only, as the latter does not apply to the EPO) and classifies potential clauses in terms of their importance for the conclusion of the DPA.
- Dedicated **workflows**, which aim to offer a visual explanation of the interactions between different instruments of the risk management package and their indicative implementation over time.

Figure 3: Transmission and transfer under the DPR



Source: DPO

These instruments support the assessment and management of the risks associated with processing personal data, especially when sharing personal data with other public entities or outsourcing services to external providers.

8. Data protection: compliance framework

In accordance with Articles 42, 43 and 47 DPR, both the DPO and DPB monitor the compliance of the processing operations with the DPR. In addition, the DPO conducts data protection audits and inspections and makes recommendations to the controller following their respective results and findings (Articles 43(1)d. DPR and 43(2) DPR).

In 2022 the DPO prepared a comprehensive data compliance framework that covers data protection self-assessments, audits and inspections.

8.1 Data protection audits

Data protection audits conducted by the DPO serve to formally monitor compliance with the DPR in terms of both documentation and implementation. They also mitigate risks for the organisation connected with irregularities, non-conformities, violations, suggestions for improvement and noteworthy efforts by enabling the delegated controllers and the President of the EPO or the President of the Boards of Appeal, as the controller, to put in place preventive, mitigating and/or corrective measures.

From a governance point of view, regular data protection audits also give the EPO with a clear indication of its compliance with the DPR, while highlighting its best practices in managing personal data, which can subsequently be extended to other areas, creating a positive continuous improvement loop. The audits are also a mechanism to put into effect the accountability principle and their results serve as additional evidence of efforts to continuously guarantee and ensure

compliance with the DPR and demonstrate it to data subjects. They may also serve to highlight other risk areas and increase awareness of data protection compliance in general.

Data protection audits will be planned in advance and included in an annual audit plan approved by the EPO President. In 2023, four audits are formally foreseen.

8.2 Data protection inspections and ad-hoc compliance queries

Under Articles 43(1)d and 43(2) DPR, any body set up under the legal provisions of the European Patent Organisation (including the DPB), or any individual subjected to processing activities carried out by the European Patent Office may request the DPO to investigate matters and occurrences directly relating to the DPO's tasks.

Data protection inspections are triggered by a specific request/at the mandate of the EPO, e.g. by the President, the President of the Boards of Appeal, a delegated controller, or an EPO statutory body, including the DPB, or initiated on its own initiative by the DPO based on repetitive complaints or other justifying occurrences under a risk-based approach. Ad-hoc data protection compliance queries, by contrast, may be required to analyse and respond to internal and external consultations, and/or complaints that cannot be channelled through the legal redress mechanisms because they do not directly impact the rights of the complainant. Both procedures may identify instances of incompliance (irregularities, non-conformities or violations of the DPR). In such cases, the DPO can recommend preventive, mitigating or corrective measures.

8.3 Data protection self-assessments by the delegated controller

Data Protection self-assessments constitute a supplementary compliance and risk management instrument for ensuring regular and on-the-spot evaluation of the compliance of processing operations in the delegated controllers' organisational units. Data protection self-assessment is carried out under the responsibility of the delegated controller on the basis of, among others, the data protection principles and requirements, elements for improvement highlighted in data protection audits, and factors like the sensitivity of the processing activities in the specific area and the number of complaints and personal data breaches experienced.

9. Communication, training and awareness raising

A new series of data protection **e-learnings** for EPO staff was launched in 2022, including e-learning modules on processing personal data within the scope of the tasks of the EPO, on data breaches, on data subject rights and on the accountability principle in data protection.

The DPO supported several units (Principal Directorate Co-operation and Patent Academy, Principal Directorate Internal Audit and Professional Standards, as

well as Appeals Committee Secretariat) to organise tailor-made data protection training for their staff in 2022.

Specific training courses on the risk management package and its instruments were provided to the data protection liaisons and BIT Privacy and Procurement.

A joint conference on social media ("Embracing social media in your organisation: benefits and privacy challenges") was organised by the DPO with the support of Principal Directorate Communication and in co-operation with the European Centre On Privacy and Cyber Security (ECPC) of Maastricht University in 2021 and with the European Intellectual Property Office (EUIPO) for all staff in September 2022.

To reflect the DPO strategy and provide staff and managers with useful resources to help them fully understand their rights (as data subjects) and obligations (as delegated controllers/processors) in relation to the protection of personal data, the content of the DPO's intranet homepage was regularly updated in 2022.

Furthermore, the advisory activity of the DPO played a very important role in the continuous awareness raising process by providing clarification and guidance on how to interpret the relevant rules.

Numerous DPO publications form part of the awareness-raising strategy devised by the DPO in 2022. Some of these publications are outlined below.

9.1 Explanatory note on the role of external providers when processing EPO personal data

The explanatory note aims to give a brief outline of the application of the DPR concepts and provisions to scenarios where private service providers process EPO personal data, i.e. where these are processors or autonomous (or independent) controllers. Furthermore, it endeavours to clarify the obligations of the EPO as controller whenever outsourcing services involving personal data sharing and offer guidance on potential DPR interpretations for external service providers. It also explains the DPO's interpretation of the position of the EPO before private service providers that may not consider themselves as processor with respect to the processing of the EPO's personal data, and seeks to offer guidance on how to apply the DPR when interacting with external private entities.

9.2 Confidentiality assessment for records of processing activities

This assessment aims to provide guidance for delegated controllers in assessing whether a record of processing activities can be considered as confidential and thus, should not be published in the Data Protection Register. It establishes the key considerations that must be present in the delegated controller’s assessment to ensure compliance with the Data Protection Rules. Under the DPR, the controller needs to maintain a record of processing activities, which should at least contain the information listed in Article 32(1) DPR. These records are kept in the Data Protection Register, which is publicly available (Articles 32(4) and (5) DPR), with the exception of any confidential records (Article 32(6) DPR). In compliance with the transparency principle and data subjects' right to be

informed, all records should be published. In exceptional cases, records may be classified as confidential and exempted from publication. Therefore, this document aims to establish an exhaustive checklist enabling delegated controllers to assess whether, in compliance with the principles enshrined in the DPR, a record may be considered as confidential.

9.3 Summary table on data sharing instruments - transmission, transfer and derogations

The DPR foresee three main instruments for sharing personal data outside the EPO, which consist of: transmission (Article 8 DPR), transfer (Article 9 DPR) and derogations (Article 10 DPR). The use of these instruments depends on the nature (public or private) and the role (processor or not) of the recipient, its location and the legal framework that it is subject to, and the purpose of the processing. As using these instruments can be complex, the DPO prepared a table summarising when each of the different concepts apply and which safeguards and measures (e.g. data protection clauses, data processing agreements, administrative arrangements) must be used in the different cases to ensure that the personal data are adequately protected and the rights and freedoms of data subjects are safeguarded when sharing personal data with external entities.

9.4 Data protection guidance and recommendations on data subjects' rights and DPR concepts

The DPO aims to issue guidance and recommendations about Data Protection Rules' provisions and concepts and data subjects' rights provided for in the DPR. In 2022, the DPO published the following guidance and recommendations:

- Data Protection Guidance on Data Protection Principles (Article 4 DPR) and Legal Basis (Article 5 DPR) offers practical advice to delegated controllers on the key data protection principles and lawful grounds for the processing of personal data.
- Data Protection Guidance on processing for another compatible purpose (Article 6 DPR) provides hands-on recommendations to delegated controllers regarding the interpretation and application of the concept of compatible further processing of personal data under Article 6 DPR and in the assessment of compatibility.
- Data Protection Guidance and Recommendations on the Processing of Personal Data under Articles 11 and 12 DPR offers guidance on the principles that apply to processing of special categories of personal data.
- Transparency and modalities for the exercise of data subject rights and the right to information provides practical advice to delegated controllers on the interpretation and application of Articles 15-17 DPR.
- Data Protection Guidance on right of access (Article 18 DPR) offers hands-on recommendations to delegated controllers on handling access requests by data subjects.

This exercise will be continued in 2023.

10. Data Protection Board

The Data Protection Board (DPB) introduced by the DPR is an external body with supervisory and advisory functions and is part of the mechanism for legal redress under Article 50 DPR.

Together with the DPO, the DPB monitors that the fundamental rights to privacy and data protection are observed when personal data are processed by the EPO.

To this end, the DPB provides independent, effective and impartial oversight of the application of the relevant provisions and examines complaints lodged by staff - current and former - and external data subjects on data protection issues.

Moreover, the Data Protection Board issues an opinion on the need for a data protection impact assessment following a request from the controller; establishes a list of the kind of processing operations that may require a data protection impact assessment and those that do not; and provides consultation and written advice to the controller on various issues.

To carry out their duties and exercise their powers, the Data Protection Board and the Data Protection Officer are granted independence from internal and external interference. In 2022, the Chair, the two members, and one alternate member of the Data Protection Board were appointed for a renewable mandate of three years.

The DPB examines complaints lodged by staff and external data subjects on the application of the EPO Data Protection Rules, thus providing a timely, fair and independent legal redress mechanism, consistent with fair trial principles. No complaints were lodged by data subjects in 2022.

In co-operation with the DPB, the DPO prepared workflows based on the DPB Rules of Procedure to facilitate co-operation between the DPB and the EPO.

Throughout 2022, the DPB formally adopted its first opinions, such as the Opinion 2/2022 of the Data Protection Board on Data Protection Impact Assessment Lists pursuant to Articles 38(5) and 47(2)(b) DPR, which complements the risk management package.

11. DPO advisory activities and business support

As set out in the DPR, the DPO monitors the EPO's processing of personal data to ensure it observes the rules and is unlikely to adversely affect the rights and freedoms of data subjects. The DPO's tasks in this area range from advance consultation on processing operations likely to present specific - and, especially, significant - risks to those rights and freedoms, to handling requests and complaints, and carrying out data protection inspections and audits aimed not only at correcting irregularities and non-compliance, but also at providing recommendations on preventing them in the future.

The advisory activity of the DPO is both of a strategic and a practical nature. On the one hand, the DPO is involved in a consultative capacity in almost all major EPO projects, initiatives and activities, to analyse the data protection aspects with a view to ensuring data protection by default and by design. On the other hand,

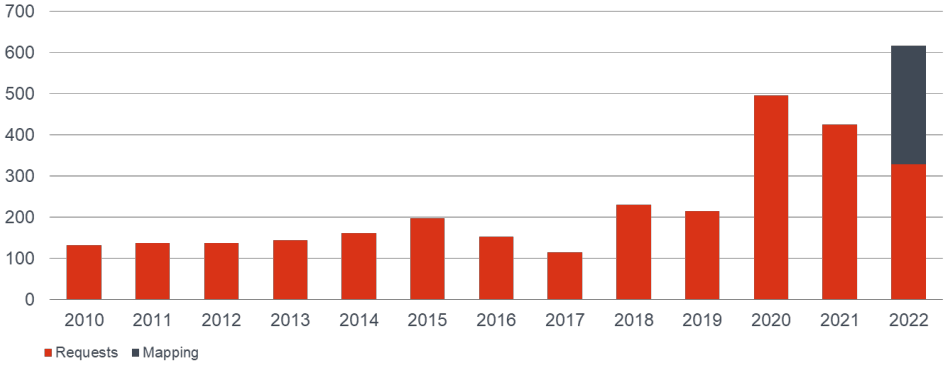
the DPO is also supporting operational units to address and resolve data protection issues regarding their day-to-day business.

11.1 Day-to-day consultations

The advisory role of the EPO in day-to-day activities is highlighted by the consistently high number of consultations. In the course of 2022, the DPO responded to 617 consultations in total, versus 425 in the previous year. This significant increase compared to 2021 (+45%) was due, among other factors, to the high number of consultations (289) related to the verification of data protection documentation (records of processing operations and data protection statements) drafted by the DPLs.

In the course of the above-mentioned consultations, the DPO issued to delegated controllers a significant number of legal opinions, of which 29 interpretative Opinions pursuant to Art 42(7) clarifying the application of the DPR.

Figure 4: Evolution of the number of requests to DPO



Source: DPO

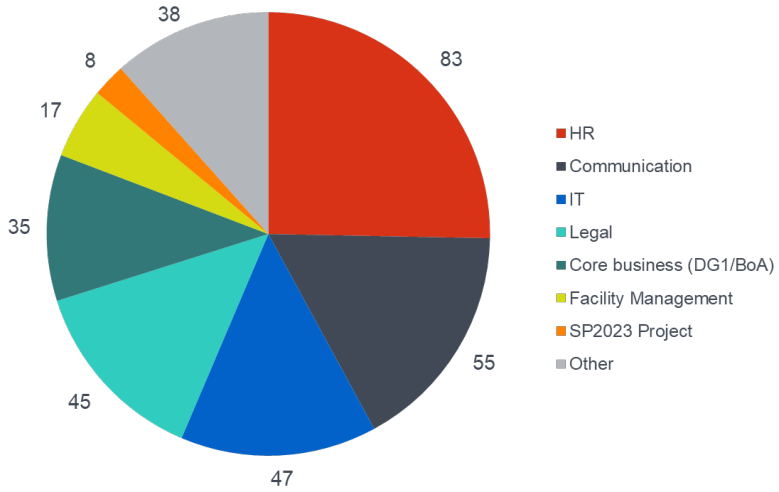
The chart above underlines an increasing trend with consultations received over the years by the DPO from the EPO's units. As a result of awareness raising on data protection issues, the EPO's delegated controllers have become increasingly competent in the due manner of demonstrating compliance and accountability in terms of privacy and data protection.

The operational documentation issued by the DPO (including work instructions, quick guides, checklists, templates, manuals, etc.) covers a broad spectrum of practical aspects that are useful for the DPLs and the delegated controllers when addressing the more ordinary cases, meaning that generally only the more complex issues are submitted to the DPO for advice.

Moreover, the awareness campaign and training provided to EPO staff and the extensive information and guidance available on the DPO intranet pages offer useful resources that help staff and managers to understand key data protection concepts and have contributed to reducing their need to consult the DPO on simple questions.

The pie chart below shows the nature of the consultations received by the DPO in 2022.

Figure 5: Requests to DPO – breakdown by nature of consultation



Source: DPO

The DPLs are increasingly becoming the first point of contact for their respective organisational units and also liaise between the DPO and the delegated controller.

It is foreseen that the role of the DPLs in advising on day-to-day activities will continue to grow in the future, and that the number of consultation requests submitted to the DPO by the delegated controllers and their DPLs on more complex issues will stabilise in the coming years.

11.2 Verification of data protection documentary compliance and data subject request consultations

Verifying the documentation (records and data protection notices) prepared by the delegated controllers (supported by the DPLs) in terms of their compliance with the requirements laid out in the DPR was one of the DPO's key advisory activities in 2022 with a total of 289 recorded consultations.

Besides supporting individuals and delegated controllers, the DPO was also consulted on seven data subject requests (five access requests and two deletion requests).

12. Personal data breach management

By definition, a personal data breach is a security incident involving personal data that compromises the confidentiality, integrity or availability of the personal data involved. Examples include the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data stored, transmitted, or otherwise processed.

A personal data breach can have a variety of serious negative effects for individuals, which may result in physical, material or non-material damage. These can include loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data

protected by professional secrecy or any other significant economic or social disadvantage for the affected individuals.

In accordance with the data protection rules, controllers are required to promptly address any data breaches, including properly evaluating, mitigating and notifying the DPO as well as, in some circumstances, communicating the breach to the individuals affected too, so they can take protective measures.

To this end, the DPO issued a complete data breach manual, as well as a quick reference guide answering the most frequent questions on this topic and a personal data breach report template. They offer guidance on managing and handling personal data breaches with a view to evaluating these risks, based on the potentially adverse effects on the rights and freedoms of the data subjects, and implementing appropriate technical and organisational measures to address them.

During the reference period for this report, the DPO investigated nineteen data breaches. After analysis by the DPO together with the respective delegated controller, it was concluded that, based on the objective assessment of the potential risks to the individuals, on both the likelihood and severity of the risks to the rights and freedoms of the data subjects, the respective risk varied between "low or no risk" (thirteen cases) and "medium risk" (two cases), with four classified as "high risk" and none as "very high risk".

The data breaches occurred either due to human error or to a bug detected in the IT system, which led to a confidentiality, availability and/or integrity breach of personal data processed by the EPO. Relevant remedial action and preventive measures were prescribed to be put in place by the respective delegated controller to address each breach and avoid similar breaches in the future.

For the analysis and elaboration of the reports, the DPO applies a widely used methodology approved by the European Data Protection Supervisor (EDPS) and other national data protection authorities, while following the procedure for addressing personal data breaches, including an escalation mechanism.

13. Co-operation with network of counterparts at international organisations and the EDPS

As in the previous years, the DPO participated in numerous initiatives in co-operation with other international organisations and European Union Institutions.

After having been invited to become a member of the Data Protection as a Corporate Social Responsibility research project launched by the European Centre on Privacy and Cybersecurity of Maastricht University in 2021, the EPO became a permanent member of the Corporate Social Responsibility Stakeholders Group in 2022, reflecting its commitment to data protection and its crucial role in the digital society.

The group's goal is to continue to successfully translate theoretical ethical principles into tangible, practical guidelines to build a solid framework for organisations to apply to foster transparency, accountability, fair, secure and sustainable data processing activities that positively contribute to the greater good.

Other co-operation activities in which the EPO DPO was involved in 2022 include:

- Annual workshop on data protection within international organisations, launched and hosted by the EDPS, in which potential common legal instruments to regulate transfers from European Union institutions to international organisations and *vice versa* are discussed.
- Working group with other international organisations' DPOs to elaborate a proposal for standard contractual clauses (regulating transfers between international organisations and private (commercial) entities located in the European Economic Area) where the observance of international organisations' legal status and consequent conditions (in particular, privileges and immunities) are specifically recognised.
- At its request, the DPO was granted the opportunity to attend the regular meetings between the EDPS and European Union institutions DPO network as an observer. This means that the DPO will remain fully up-to-date and aligned with any developments in European Union data protection-related policies and procedures. The invitation also demonstrates the importance of the EPO's DPO efforts and reflects the recognition it enjoys on the part of European Union institutions and the EDPS.

As part of the activities outlined in the Annual Work Plan approved by the EPO and the EUIPO, quarterly meetings took place in 2022 between the two offices' DPO teams. Until now, the EPO and EUIPO have collaborated to develop a data protection clause assessment tool, which aims to help data processing agreement reviewers (e.g. DPLs) to assess clauses in accordance with the applicable regulation, data protection audit framework and transfer impact assessments. A conference on data protection and social media was also jointly held by the EPO and EUIPO DPOs.

Moreover, both DPOs participated in the aforementioned task force on international transfers launched by the EDPS. Additionally, the EUIPO, together with the European External Action Service "EEAS", presented a draft administrative arrangement to cover the transfer of personal data from European Union institutions to international organisations.

Comments were submitted by international organisations, including the EPO. The results of this collaborative task force may lead to the preparation of specific provisions and the implementation of adequate safeguards for the transfer of personal data between the EUIPO and the EPO, thereby supporting fully data protection-compliant co-operation between the offices.

14. Future challenges

After having laid down the new legal framework in 2021 and guided and monitored its organisational and practical implementation in 2022, the DPO will look at the institutional framework, creating new rules and setting up mechanisms and procedures to create institutional cohesion; and ensure that the same data protection principles are applied across the European Patent Organisation.

The DPO aims at becoming the DPO for all organs, bodies and committees of the European Patent Organisation and protect the rights and freedoms of all data subjects, regardless of which subsidiary body or organ of the Organisation processes their personal data.

In 2023, particular attention will be paid to the data protection aspects of the functioning of the Boards of Appeal and the Administrative Council.

In line with the EU data protection rules, data processing by the Boards of Appeal in their judicial capacity is subject to the Office's data protection framework yet excluded from the oversight and legal redress mechanisms that the DPR puts in place for data processing by the EPO. The DPO will therefore support the Boards of Appeal in creating appropriate oversight and legal redress mechanisms.

Together with the Secretariat of the Administrative Council and the Office's legal services, the DPO has also been working to establish a legal framework for the processing of personal data by the Administrative Council and the transmission of personal data between the EPO and the Council, which falls into line with the envisaged streamlining of governance mechanisms.

The DPO will also continue its efforts to raise staff awareness of the mechanisms and measures put in place by the EPO to protect their data, ensuring they understand the impact of the design, evolution, risks and deployment of technology and policies on their fundamental rights to privacy and data protection. With a view to raising awareness, additional training modules will be developed, together with further e-learnings on specific topics.

Starting in 2023, the DPO will review a selection of personal data processing operations from the EPO Data Protection Register to verify whether they comply with requirements laid down in the DPR relating to documentation and implementation. This data protection audit exercise will aim to establish the ratio of personal data processing operations verified by the DPO that have been found to comply with the requirements of the DPR.

The DPO will continue to integrate privacy and data protection into all areas of the EPO's work and in co-operation with all departments.

The risk management instruments developed to support the progressive compliance of the EPO's processing operations with data protection principles will enable implementation of the principles of data protection by design and by default with a risk-based approach.

2023 will also see the continuation of the DPB's work. The DPO will continue to support this official body in its supervisory tasks, enabling it to handle any complaints from staff or external data subjects independently.

2022 was the year of the framework's implementation, in which all required operational changes stemming from the new legal framework were put in place. It also saw the set-up of the EPO's data protection community, which is defined by values, not frontiers, and opportunities, not obstacles.

Ruled by this credo, the EPO and its DPO will continue to invest resources and efforts in finetuning and enhancing the EPO's data protection framework to promote privacy and data protection in all of its areas, activities, initiatives and projects.

In 2023, the remaining actions of the DPO Strategy and Planning 2021-2023 will be delivered and the DPO will prepare its Strategy and Planning 2024-2026 to set out how the EPO intends to achieve sustainable privacy and data protection.