Europäisches Patentamt
European Patent Office
Office européen des brevets

Data Protection Report 2020

Executive summary

With an increasing amount of personal data online and cybercrime on the rise, data protection is more than just a legal obligation for the EPO. It's a matter of integrity and preserving the trust placed in the organisation by its staff and users. Empowering individuals to take control over how their personal data is processed is of paramount importance to the EPO.

Although not bound by the EU's data protection legislation, the EPO's decision to align its data protection rules with the principles and key requirements of the General Data Protection Regulation (EU) 2016/679 and Regulation (EU) 2018/1725 reflects the organisation's clear commitment to adopt and comply with the highest standards.

EPO data protection programme: anticipation, action, unity – working together to protect privacy and personal data

State-of-the art data protection is also a key objective of the EPO's ambitious data protection programme, as set out in its Strategic Plan 2020-2023. The main pillars of this programme are anticipation, action and unity. Because, for the EPO, effective data protection is not only about foresight and adopting best practices. It's about creating a shared sense of responsibility that arises from the collective efforts of all internal stakeholders.

In 2020 the EPO began the groundwork that will lay the foundations for its new best-in-class data protection framework. To this end, a network of Data Protection Liaisons was created and senior managers were offered in-depth training on data protection. Last year also saw the launch of a large-scale exercise to map personal data processing across the organisation. This was accompanied by a first draft of new data protection rules based on input from all internal stakeholders.

Work on these new data protection rules, along with a host of other initiatives, will continue in 2021. Ultimately, by achieving compliance with the highest international standards and linking it with fundamental ethical principles, the EPO aims to turn data protection into a competitive advantage.

Contents

1. Introduction

The Guidelines for the protection of personal data in the European Patent Office (DPG) were adopted on 19 March 2014.

The DPG set out the principles and rules applicable to data protection at the EPO and define the role and responsibilities of the Data Protection Officer (DPO) in monitoring, supervising and assisting with their implementation to ensure that they are duly applied.

Under Article 19(6) DPG, the DPO is required to submit an activities report to the EPO President each year.

This report gives an overview of the DPO's activities in 2020, focusing on the beneficial results achieved for the EPO and on the upcoming challenges.

2. Data Protection Officer's role and responsibilities

The duties of the DPO and the DPO's Deputies and the details of their appointment are governed in Articles 18 to 20 and 23 to 25 DPG.

The DPO has responsibility for ensuring that the EPO respects the fundamental rights to privacy and data protection, be it when processing personal data or in developing new policies, procedures and practices. In general terms, the DPO has the following remit:

- **Organisation, monitoring and supervision**: the DPO monitors the EPO's processing of personal data to ensure it is in observance with the DPG and unlikely to adversely affect the rights and freedoms of the 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 inquiries. The DPO also manages the network of Data Protection Liaisons (DPLs) responsible for first-level monitoring of whether personal data processing operations carried out as part of their business units' activities, projects and initiatives comply with the requirements of the DPG and verifies whether they are performing this and other tasks efficiently.

- **Consultation**: the DPO advises the EPO President, the delegated controllers and the processors on matters related to interpretation and application of data protection requirements generally. The DPO may be directly consulted by the President, the delegated controllers, any body set up under the EPO's Service Regulations and any individual on matters related to the interpretation or application of the DPG in particular.

- **Training, information and awareness-raising**: the DPO promotes and raises awareness of privacy and data protection matters throughout all the areas of the Office. Besides contributing to the EPO's learning strategy to ensure that it includes adequate training on protecting personal data, the DPO offers a range of targeted training to the various audiences concerned, e.g. DPLs, delegated controllers, processors and internal and external data subjects (i.e. staff and users).

DPO responsibilities:

Management and supervision

Consultation and advice

Training, information and awareness-raising

Co-operation and harmonisation of practices

- **Co-operation**: as regards contacts with other international organisations, the DPO is part of a network including counterparts from e.g. CERN, the EMBL, ESO, ESA, the ECMWF, the EUMETSAT and the IARC. The DPO also participates in activities under the work programme for international organisations of the European Data Protection Supervisor (EDPS) and attends the annual Workshop on Data Protection within International Organisations. In 2019, the EPO and the EUIPO signed a memorandum of understanding envisaging a collaborative operational implementation of their closely aligned data protection frameworks and joint drafting of templates, guidelines and training programmes. Their DPO teams meet regularly to work towards achieving the highest possible standard of data protection, based on compliance with the latest developments in related EU requirements, in order to enhance both institutions' transparency and accountability towards their stakeholders.

Figure 1 – Data Protection Officer's role and responsibilities

Source: EPO

3. Main objectives in 2020

The EPO's creation of a new Directorate Data Protection Office in its Directorate General 0 Presidential Area as of 1 January 2020 reflects the importance it attaches to protecting personal data. This new position within the organisation means that the DPO reports directly to the President, which ensures independence from the operational business units.

To implement the EPO's Strategic Plan 2020-2023 (SP2023) – and, more specifically, as part of Key initiative 3 "Improve transparency and accountability" of its Goal 5 "Secure long term sustainability" – the President approved a tracked activity mandating the DPO to oversee the revision and implementation of an improved data protection policy at the EPO.

Initiated in 2020, this revision process involves updating the existing DPG by enshrining the data protection concepts, principles and requirements laid down in the EU data protection legislation (General Data Protection Regulation (EU) 2016/679 and Regulation (EU) 2018/1725) and, based on the benchmarking against other international organisations done to date, aligning the EPO's data protection framework with the "best in class" among them.

The pillars of the new modern and efficient EPO data protection framework are:

1. The creation of a comprehensive Data Protection legal framework, including the new Data Protection Rules, data protection related policies, instructions and documentation, to constitute a solid legal basis for the EPO to conduct its processing operations in compliance with the highest standards and in full transparency and respect of the data subject's rights.

2. Data Protection operational compliance through the setting up of measures and mechanisms to safeguard transparency and ensure compliance, including the mapping of the existing processing operations and the creation of the new data protection registry.

3. Risk management and mitigation, with the creation of a new body with overseeing and advisory function, and the implementation of further monitoring and detection mechanisms (data protection audits and investigations) and of specific procedures to address and mitigate data breaches.

4. Risk prevention through awareness raising on the obligations of the delegated controllers and the processors.

5. Continuous improvement, through the steady cooperation with other International Organisations and public institutions, and the exchange of best practices, the DPO ensures that the EPO, in line with its goal of long-term sustainability, remains abreast of technological innovations and transformation in the area of data protection and privacy.

DPO objectives in 2020 and going forward:

Data protection legal framework

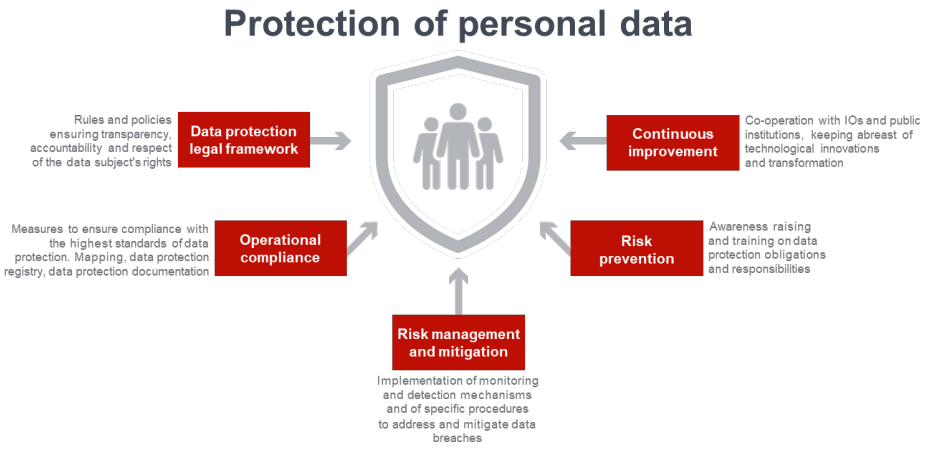
Operational compliance

Risk management and mitigation

Risk prevention

Continuous improvement

Figure 2 – Pillars of the new EPO data protection framework



Source: EPO

4. Milestones and achievements in the area of data protection

4.1 Corporate data protection framework

New EPO data protection framework: preparation

The DPO drafted the documentation for SP2023 tracked activity 5.3.0 on revising the EPO's data protection policy and circulated it among the members of the EPO Management Advisory Committee (MAC), staff representatives and the Boards of Appeal. The President approved it in the summer of 2020. The DPO carried out a complete analysis to define the exact scope and nature of the operational adjustments to be made by the EPO's delegated controllers in their respective business areas. The DPO started revising the DPG in wide consultation with all relevant internal stakeholders, with a view to submitting the EPO's new Data Protection Rules to the Administrative Council for adoption in June 2021.

4.2 Establishment of a Data Protection Liaisons network

Data Protection Liaisons: first point of contact for the EPO's operational units

To facilitate effective and harmonised data protection compliance by the various stakeholders at the EPO, the DPO set up a network of Data Protection Liaisons (DPLs) to ensure the DPO is properly involved in good time in all processing of personal data at the EPO. These DPLs will also act as a first point of contact for the EPO's operational units when they have questions about privacy and data protection.

The appointed DPLs were given in-depth initial training offered by external providers specialised in data protection.

In preparation for the launch of the mapping/inventory exercise to identify, verify and formalise all the processing of personal data taking place in the EPO's business units, the DPLs were also provided by the DPO with the necessary training, background information and model documentation to enable them to initiate and carry out this exercise in their own operational units. Regular bi-weekly meetings were held to discuss the challenges, provide continuous training and support the DPLs in the performance of their tasks.

4.3 New data protection tool

New EPO data protection tool

A new tool will make it easier to technically manage implementation of the revised legal framework for data protection to be introduced under the SP2023. It will comprise various operational modules, including data mapping, risk assessment automation, privacy incident response and website scanning for cookie consent and compliance. Over the course of 2021, the DPO (while gradually delegating the task to the newly nominated DPLs) will work together with the delegated controllers on drawing up the documentation (records and data protection notices/statements). It will then be reviewed for compliance in terms of the accuracy and completeness of the defined "commitments". A further DPO "check" will then verify whether those commitments have been observed during practical implementation.

4.4 Comprehensive mapping of processing operations

Mapping of EPO processing operations

The inventory and mapping of the EPO's personal data processing operations started in Q3 of 2020 and will result in the creation of a complete and accurate Data Protection Register recording all such operations. This Register is one of the key prerequisites for guaranteeing the EPO's accountability in terms of data protection.

Every year from 2022 onwards, the DPO will review a sample of personal data processing operations from the Register – selected in a risk-based approach – to verify whether the "commitments" declared in the related records comply with the requirements laid down in the data protection and privacy rules in terms of their accuracy and completeness and whether they have been observed during practical implementation.

4.5 Advisory activities

As set out in the DPG, the DPO is available to provide the delegated controllers/DPLs with any support they might need and is also required to carry out an *ex-ante* review of processing operations.

Daily consultation and advice

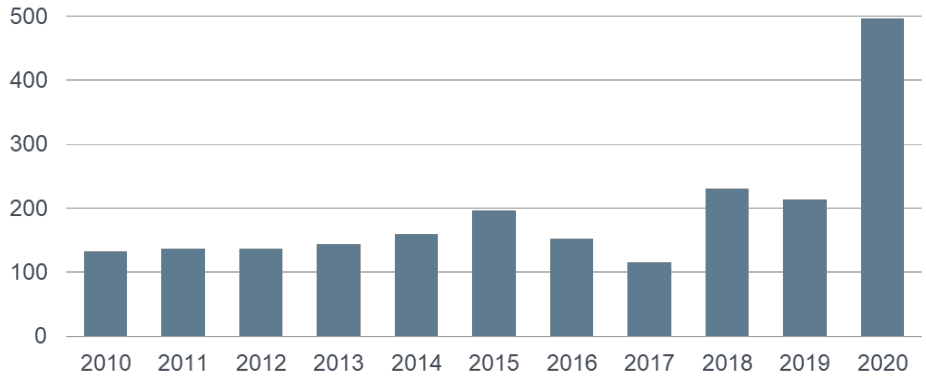
The number of requests for consultation submitted to the DPO in 2020 was more than double that received in 2019. By the end of the 2020 working year, the DPO had responded to 494 consultation requests, including some of considerable complexity, which is an increase of 131.92% over the previous year.

The table below shows the total and quarterly figures for requests for consultation submitted to the DPO in 2020 and how they compare with the 2019 figures.

Year + quarter	Number of requests to DPO	Comparison
2020 – Q1	60	-9.09%
2020 – Q2	205	+236.07%
2020 – Q3	99	+147.50%
2020 – Q4	130	+182.61%
2020	**494**	**+131.92%**
2019 – Q1	66	
2019 – Q2	61	
2019 – Q3	40	
2019 – Q4	46	
2019	**213**	

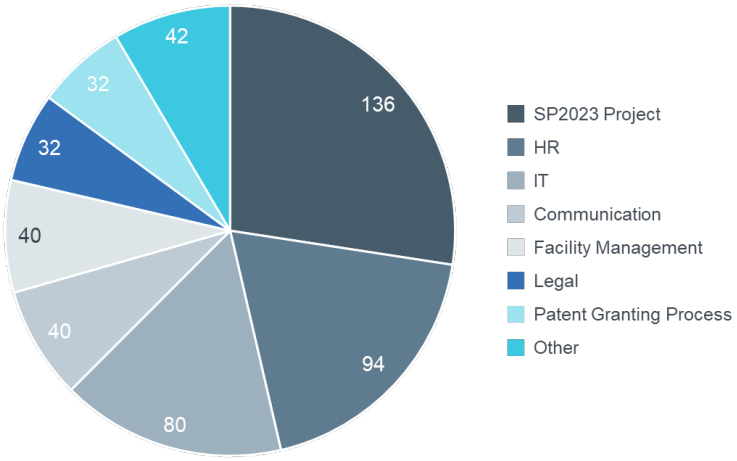
The graph below shows how the number of consultation requests has developed over the course of the last few years. The growing number of queries shows that the EPO's delegated controllers are becoming ever more aware of the importance of demonstrating compliance and accountability in the area of privacy and data protection. The DPO is involved routinely – and generally in good time – whenever there are questions/doubts about the processing of personal data.

Figure 3 – Yearly overview of requests to Data Protection Office



Source: EPO

Figure 4 – Requests to Data Protection Office in 2020: breakdown by area of origin



Source: EPO

4.6 Awareness raising

In 2020, the DPO conducted an active campaign to guarantee that both those who work at the EPO and, indirectly, its users, external stakeholders and partners could gain not only a better understanding of the applicable data protection requirements but also a heightened awareness of the risks associated with processing personal data and the safeguards which therefore need to be put in place.

Training, information and awareness-raising

Within the EPO, the DPO focused on encouraging, expanding and strengthening a culture of transparency and accountability. This involved providing the DPLs, managers and staff with the knowledge and instruments they need to go beyond simple formalistic compliance and ensure that they are also able to effectively demonstrate this compliance.

In 2020 the DPO launched various initiatives to raise awareness of privacy and data protection among EPO staff and management: specific training (online training event with speakers from Maastricht University's European Centre on Privacy and Cybersecurity); presentations to the MAC members, top management from the majority of the business units and all SP2023 project managers and DPLs; and general and thematic training, e.g. an introduction to basic data protection concepts and the applicable legal basis and principles and sessions dedicated to international data transfers, privacy and security risk assessments and data protection impact assessments.

Further targeted training and communication campaigns to raise awareness among staff at directorate-general/directorate/business unit level will take place in 2021.

The content of the DPO's intranet pages was revised to reflect the DPO strategy and provide staff and managers with useful resources to help them become fully aware of their rights (as data subjects) and obligations (as delegated controllers/processors) in relation to the protection of personal data, understand the key notions and principles of data protection and access quick guides on everyday issues ("do's and don'ts").

The DPO will also initiate and manage an update of the content of the data protection notice on the EPO website to ensure it provides external data subjects (users, partners and stakeholders) with all the "must have" information on the special features of the EPO's processing of personal data and on its adherence to the principles of compliance and accountability.

4.7 Data breaches

In 2020 DPO introduced an operational procedure to be followed at the EPO for investigating and tackling security incidents which might have an impact on personal data.

Personal data incident management

During the reference period for this report, the DPO investigated five personal data breaches. In those cases where the DPO's analysis, carried out together with the delegated controllers concerned, confirmed the breach, it was concluded that, based on an objective assessment of both their likelihood and severity, the potential risks involved for the rights and freedoms of the individual data subjects varied from "none" to "medium".

The confirmed cases involved an integrity and/or confidentiality breach of personal data processed by the EPO resulting from either human error or a bug detected in IT systems.

In each case, the delegated controller concerned was informed of both the remedial action to be taken to address the breach and preventive measures to avoid similar breaches in the future.

For the analysis and the drawing up of the reports, the DPO applied a best practice methodology approved by the European Data Protection Board ("EDPB") and the EDPS and followed the procedure for addressing personal data breaches, which includes an escalation mechanism.

The DPO is in the process of drafting a complete manual on managing and handling personal data breaches with a view to putting a formal procedure for this in place at the EPO. The manual will set out how the various roles and responsibilities are to be assigned, the steps to be followed to ensure a proper investigation and what follow-up measures/actions need to be taken. The DPO will conduct the training required by those involved in this procedure.

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

Co-operation and harmonisation of practices among international organisations

The DPO co-operated with a network of counterparts at other international organisations and the EDPS to arrive at a common understanding and interpretation of data protection standards, thereby ensuring that appropriate procedures and tools can be put in place to support implementation of the EPO's new Data Protection Rules and related guidance documentation, as reviewed and updated to reflect this understanding. The DPO also profited from this international network as a forum for launching several initiatives aimed at identifying synergies and achieving greater harmonisation of policies and procedures and improved dissemination of best practices.

The annual Workshop on Data Protection within International Organisations, launched and hosted by the EDPS, took place on 8 and 9 October. The DPO was specially invited by the EDPS to give a presentation on the topic of transfers on the second day and a workshop session was dedicated to reporting on new developments and best practices in facilitating transfers to international organisations. The participants also discussed digital transformation and governance, this being an urgent priority due to the COVID-19 pandemic given that digital technologies and data have a valuable role to play in combating the crisis.

Mobile applications typically installed on smartphones (apps) can support both public health authorities and international organisations in monitoring and containing the COVID-19 pandemic and are particularly relevant in the phase of lifting containment measures.

The DPO launched two initiatives involving other international organisations in 2020:

- in response to a call for interest issued by the DPO, a number of international organisations' DPOs came together as an informal working group to share their observations and questions on the EDPB Guidelines 2/2020. This discussion was considered necessary in view of the expected consequences of the Guidelines for the transfer of personal data between EEA public authorities/bodies and international organisations and for any further transfers of this data by international organisations. The DPO analysed the input received and shared a summary of the results with the EDPS. This led the EDPS to hold a specific session on the matter during the annual Workshop on Data Protection within International Organisations and to invite

the DPO to be one of the speakers. The EDPS followed this up by issuing a call for interest among international organisations in creating a task force on the topic of international transfers. The DPO welcomed this and expressed interest in participating.

- following another call for interest issued by the DPO, a number of international organisations agreed that the DPO should request the EDPS to set up the planned task force on international transfers and should explore, together with the EDPS and/or the EU Commission (International Data Flows Unit), the possibility, firstly, of establishing a common mechanism to regulate inward and onward transfers (from the EU Member States) made to and by international organisations for the purposes of performing their mandate, duties and responsibilities and, secondly, of jointly drafting a model data processing agreement (standard contractual clauses) specifically targeting the transfer of personal data by international organisations to processors in third countries.

In addition, the DPO has been invited to join the IGOPA, a working group specifically set up to carry out benchmarking among scientific intergovernmental organisations and develop best practices for their protection of personal data. The DPO expressed interest in participating in its activities and contributing to achieving its deliverables.

Lastly, the DPO was contacted by several counterparts at other international organisations who wished to express their interest in and support for the joint actions initiated by the DPO and consult the DPO on critical data protection issues commonly encountered at international organisations.

4.9 Co-operation with the European Intellectual Property Office (EUIPO)

Co-operation and harmonisation of practices with European institutions

As part of the activities envisaged in the Annual Work Plan approved between the EPO and the EUIPO on 23 June, a first meeting between the two offices' DPO teams took place on 27 November. After introducing themselves and taking a look at the responsibilities of DPOs at EU institutions and international organisations and the challenges they currently face, the teams discussed the present state of play on various crucial topics in the field of data protection, such as the negotiations in the "Microsoft" case, the remote audits of the EU institutions by the EDPS and the follow up actions on the CJEU's recent judgment in the "Schrems II" case. They also brainstormed on possible data protection synergies between the EUIPO and the EPO and the nature and scope of the joint activities to be carried out by the two institutions' Data Protection Offices in 2021, e.g. a common awareness-raising campaign and training. The next regular meeting is planned for February 2021.

5. Present challenges and risks

A number of global events affected the EU Member States and the international data protection landscape in 2020. The DPO is currently analysing the significant challenges and risks posed by these developments.

6. Conclusion

The revision of the data protection framework initiated this year and managed by the DPO as SP2023 tracked activity 5.3.0 means that the EPO has to put in place now all the groundwork necessary to guarantee its corporate and operational compliance with the new Data Protection Rules, which are planned to be adopted and implemented in 2021.

The high level of awareness among the EPO's senior managers of the importance of data protection and their strong commitment to complying with the related legislative framework will serve as the foundation for creating the right environment of effective support for the DPO's ongoing work towards closing the gaps in the existing rules and practice.

It can be expected that the DPO's due involvement, at the earliest possible stage, in all EPO projects, activities and initiatives involving the processing of personal data, along with timely consultation on the related documentation, such as contracts, policies and procedural specifications, will help to ensure that, in future, such involvement and consultation becomes a reflex action for processors and that data protection by design and default is established as a defining feature of each and every EPO operation which might have an impact on personal data.

The DPO's efforts will not end there. As scrutiny of how international organisations process personal data is likely to continue growing, protecting this data will be indispensable in ensuring the EPO's accountability and thus in safeguarding its reputation and maintaining public trust. As previously mentioned, the long-term plan is to put a new privacy and data protection framework in place which has strong backing from the management and will enable the EPO to guarantee that it embedded data protection by design. This will mean fully integrating data protection accountability into the EPO's culture so as to provide the highest possible level of protection for the data entrusted to it. This is not an easy task, but the DPO believes that the EPO is more than up to the challenge.

As a start to tackling this challenge, the DPO has submitted to the EPO President for approval a strategy and plan for 2021 to 2023 which outlines the course of action to be taken by the DPO and the EPO and the precise measures to be put in place over those three years.

DPO strategy and plan 2021-2023: working together to achieve the highest level of protection for personal data entrusted to the EPO