Data protection statement on the processing of personal data in the context of enquiries to the Ombuds Office

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.

This data protection statement relates to the processing of personal data upon enquiries to the EPO Ombuds Office in PD04 (Internal Audit and Professional Standards).

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

This data protection statement explains the way in which personal data is processed by Ombuds Office personnel and any person duly assigned when someone (beneficiary) sends an enquiry.

Personal data is processed to allow Ombuds Office personnel fulfil their function – which is to empower beneficiaries of the service to put their stalled processes back on track and to build effective working relationships for concrete, lasting improvement in the value, predictability and consistency of service delivery. For further information on the purpose of Ombuds Office please refer to the EPO.org website.

During the course of Ombuds Office activities, Ombuds Office personnel dialogue with the beneficiary of the service, explore potential ways forward with the possibility to identify and bring together the right people in an informal setting, analyse data and provide systemic and systematic insights to the relevant managerial levels in the organisation. This triggers the inevitable processing of personal data of the service beneficiaries and, depending on the case, EPO staff members of the operational units concerned by the contact and substance of the matter.

Specifically, the processing of personal data is necessary for and used to:

- log and register cases
- allow for dialogue with the service beneficiary
- monitor the evolution of the issues while the case is open with the Ombuds Office
- conduct activities to explore ways to improve the issues, including facilitating communication between the service beneficiary and, when appropriate and agreed, other functions in the EPO
- record service actions, findings and outcomes
- get insight into the process followed
- refer cases to other units when appropriate
- preparation of anonymous statistics or reports
- provide anonymous data to the President and relevant managerial levels, who can leverage the insights and findings of the Ombuds Service

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

2. What personal data do we process?

The categories of personal data that may be processed include:

- Identification data (e.g. name);
- Contact data (e.g. email address, phone number);
- Type of service beneficiary
- Description of the issue
- (when appropriate) Represented user association
- (when appropriate) Organisation/employer
- (when appropriate) The represented applicant
- (when appropriate) The application details

When contribution of another organisational unit is required, the following categories of personal data of the staff in the unit concerned are processed:

- Identification data (e.g. Name and surname)
- Contact data (e.g. Email address);
- Employment data (organisational unit)

Data contained in documentation related to the issue presented will be retained for the duration of the case with the Ombuds Office, and processed only to the extent necessary to fulfil the purpose of the processing operation as stated above. If the documentation includes data that are irrelevant to the resolution of the issue, such data will not be further processed.

In situations where the Ombuds Office receives an enquiry that falls outside its mandate, only limited categories of personal data—such as the type of beneficiary, a brief description of the issue, and the unit referred to in the response—will be processed. This contributes to the potential to obtain relevant insights. All other communications and any non-anonymised personal data will be deleted as soon as the Ombuds personnel have replied to the enquiry with the relevant information.

3. Who is responsible for processing the data?

Personal data are processed under the responsibility of the Ombuds Person acting as the EPO's delegated data controller.

Personal data are processed by the EPO staff involved in managing the initiative, project or activity of the Directorate Ombuds Office referred to in this statement.

People, both internal and external, maintaining IT systems and providing technical support may also process personal data in the course of performing their duties, with limited view access over it.

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

Personal data obtained and processed through the Ombuds Office processing operation may only be accessed on a need-to-know basis by the EPO staff working in the Ombuds Office, any person duly assigned by the data controller in support of the Ombuds Office activities, and, only to the extent that is necessary for the provision of the technical support in connection with the operation or maintenance of IT tools used for the processing operation, by staff and external contractors providing technical support to the EPO.

Disclosure of data is limited to a legal or professional obligation to do so. When disclosing, the disclosure is performed under the principles of necessity and data minimisation: Data will be disclosed on a need-to-know basis only to authorised recipients, and the detail level is restricted to the data needed for the recipient to perform their function. Whenever possible, data is shared anonymously or minimised in a way as to avoid or limit the identification of data subjects. A residual risk remains however that an individual could be identified through the circumstances described.

Specifically, disclosure of personal data is granted to the following categories of persons:

- When you raise a matter with the Ombuds Office, your data will be shared confidentially with the appropriate EPO managers, who will receive the minimum information essential to deal with your matter.
- The manager, together with the Ombuds Office and the beneficiary, may then agree whether or not and how to involve other staff members, and to what extent the beneficiary's contact with the Ombuds should be disclosed.
- In facilitating resolution and communication between the beneficiary and relevant EPO functions, the Ombuds Office applies the same confidentiality principles: all exchanges between the Ombuds Office and the beneficiary, as well as with relevant staff or managers, remain confidential unless otherwise agreed.
- When a matter highlights systemic or systematic insights, these are shared with the relevant managerial function in an anonymous manner. This action may indirectly reveal the identity of the manager concerned.

The Ombuds Office will not share aspects of the issue with other units without the prior agreement of the beneficiary or staff concerned unless any of the following situations apply:

- When the beneficiary contacts the Ombuds Office regarding a matter that falls under the mandate of another unit, and the issue requires urgent attention, the Ombuds Office may respond to the enquiry copying the relevant unit to avoid delays in handling.
- When the beneficiary exposes the issue to several EPO stakeholders to foster consistency

Ombuds Office personnel reserve the right to share any information indicating illegal activity or a risk of serious harm with the appropriate function as per Article 5(b) DPR. This includes reporting integrity issues, such as fraud, corruption or other irregular activities, to the EPO department responsible for ensuring compliance.

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.

The EPO has adopted a paperless policy management system as the default; however, if paper files containing personal data need to be stored on EPO premises, they are locked in a secure location with a restricted access.

For personal data processed in external tools, 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?

Based on Articles 18 to 24 DPR, 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.

Please note, however, that the DPR also sets certain limits to these rights:

The right to rectification (Art. 19 DPR) can only apply to factual data processed in the framework of the investigative process and applies only to objective and factual data that are inaccurate or incomplete, such as names, birth dates, addresses. It does not apply to subjective statements, including opinions or assessments made by third parties. You may, however, complement your own statement with additional clarifications and comments. Interviewed persons may also request access to the audio recording of their interview at any time in the investigative process.

Furthermore, the data subjects' rights to restriction of processing and to object (Articles 21 and 23 DPR respectively) are not equivalent to the right to remain silent on grounds relating to self-incrimination or to incriminating a close relative (Article 21a (6) ServRegs).

Please also note that the DPRs do not foresee data subject rights for individuals who are only mentioned in evidence (for example in complaints, witness statements, interviews or documents), but who are not themselves persons of interest in the investigative process.

It is also important to underline that data protection rights are not absolute and must be balanced against other fundamental rights and freedoms. This means that in some circumstances one or more rights may be refused. Moreover, under Article 25 DPR and Circular No. 420, rights may be temporarily restricted on legitimate grounds, for example where transparency would jeopardise the purpose of the Ombuds activities, affect the rights and freedoms of others, or undermine the working environment. Any such restrictions will be proportionate, time-limited and duly recorded. You will be informed individually as soon as practicably possible, unless doing so would undermine the purpose of the restriction.

If you wish to exercise any of these rights, you may contact the delegated data controller at DPOexternalusers@epo.org with details of your request. To facilitate processing, we encourage you to use the appropriate *form (for externals), this form (for internals) and/or this form (for pensioners),* and submit it with your request. We will respond 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 5a DPR, whereby "*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.*"

In case special categories of personal data are processed, the applicable legal bases are Article 5(a) DPR in conjunction with Articles 11(2) and 12 DPR.

Article 5b DPR allows staff involved in the processing operation to reserve the right to share any information indicating illegal activity or a risk of serious harm with the appropriate function and authorities.

8. How long do we keep data?

Personal data will be kept only for the time needed to achieve the purposes for which it is processed.

Once the matter with the Ombuds Office is closed, which may happen because the Ombuds Office service has been provided or because the service beneficiary informs the Ombuds Office that they do not wish to continue the procedure with the Ombuds Office, all non-anonymous personal data, including any reference to the beneficiary's organisation or affiliation, or to the applicant they are representing, will be deleted. Also, the names or information that could lead to identify the EPO staff who have been involved in the process (with exception of the concerned unit, which could indirectly lead to identify the concerned manager).

The Ombuds Office will keep anonymous records only to enable it to identify trends or systemic issues. Its reports will not contain any details which could lead to identify the service beneficiary, their company or their affiliation.

Residual personal data in the anonymous records will be deleted after 10 years after the closure of the Ombuds Office cycle. The Ombuds reports which are anonymised are kept indefinitely with the purpose to access historical data and statistical information.

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 data controller at *DPOexternalusers@epo.org.*

You can also contact our Data Protection Officer at DPOexternalusers@epo.org.

10. 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.