Data Protection Statement on the processing of personal data within the context of investigative activities

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 statement relates to the processing of personal data in the context of investigative activities conducted by the EPO Investigative Function (IF), including interviews in that context. It explains the way in which your personal data will be processed, kept and stored when you share it with the IF.

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

This data protection statement relates to the processing of personal data within the context of investigative activities conducted by the EPO Directorate Ethics and Compliance in response to allegations of misconduct against EPO Staff.

All investigative activities conducted by the IF are administrative fact-finding for the purposes of detecting and preventing EPO staff misconduct.

Personal data are processed for the following purposes:

The IF processes personal data of persons who raise an allegation of misconduct with it. Your personal data is processed for the purpose of assessing if allegations warrant investigative activities, in accordance with the internal Implementing Rules on investigations, as well as determine whether any misconduct or wrongdoing was committed. It may also be used for contact purposes.

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

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

2. What personal data do we process and how?

The categories of personal data processed for external persons making allegations to the IF are as follows:

- identification data (e.g., name);
- contact data (e.g., email address, phone number) in so far as it relates to an EPO Staff member, employment data (e.g., employment records, leave, duty travel, compensation and benefits information, performance records, disciplinary and dispute settlement information);
- case involvement data (e.g., complainant, witness, subject, observer);
- private sphere data (e.g., external activity of an EPO employee);
- evidence submitted in support of an allegation.

The personal data collected constitute an integral part of DEC's fact finding procedure. They are necessary for and used to:

- log and register cases as well as maintain case-files;
- conduct investigative activities, including interviews, and all stages of investigative processes;
- record investigative actions and reports;
- submit investigative reports for decision by EPO executives;
- refer cases to other units or to national authorities;
- inform parties to investigative processes about the outcome;
- comply with legal obligations to which the EPO is subject.

Finally, the data collected may also be processed for the management and monitoring of investigation processes, including the preparation of anonymous statistics or reports.

The data may be collected on the basis of a report by an external person, EPO employee or former employee, persons who undertake work in or on behalf of the EPO, including anonymous or confidential sources, and on the basis of publicly available information.

The data may be collected by any of the means provided in the Service Regulations and Implementing Rules, including by accessing any EPO physical or digital relevant information and documentation as well as EPO premises, and by asking oral information from any relevant person.

3. Who is responsible for processing the data?

Personal data are processed under the responsibility of Directorate Ethics and Compliance, acting as the EPO's delegated data controller.

Personal data are processed by the EPO staff involved in managing the investigative activities of the IF referred to in this statement.

External contractors involved in carrying out investigative activities may also process, including access the personal data.

4. Who has access to your information and to whom is it disclosed?

Case files maintained by the IF are only accessible by IF employees involved in investigative activities.

Personal data from the casefiles may be disclosed on a strict need-to-know-basis and to the minimum of persons to:

- EPO executives entrusted with disciplinary authority;
- EPO employees or persons who are parties to the investigative process (i.e. witness, subject, observers);
- EPO employees or persons who may be called to assist in investigative activities;
- external service providers or persons to whom investigative activities are commissioned (i.e. healthcare administrator, transcript provider, external investigator);
- EPO employees who provide legal advice (i.e. on employment law) or subject-matter
- opinions (i.e data protection);
- EPO employees who channel requests to national authorities when necessary;
- EPO employees who receive referrals from the IF for follow-up action (i.e. human resources, ombuds services);
- EPO employees or persons involved in disciplinary proceedings or legal proceedings.

Your personal data might be shared, in the framework of referrals, with competent national (law enforcement) authorities when in view of the nature of the allegations and the interests of the parties or the EPO, the case involves potential criminal offence or warrants assistance from the national authorities.

Data might also be shared, upon request, with other international institutions.

Whenever possible, the IF anonymises or minimises any such data sharing in a way as to avoid or limit the identification of data subjects. A residual risk exists however that an individual could be identified through the circumstances described.

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

Staff and external contractors providing technical support to the EPO with the IT tools used for the IF case management system may also process the personal data for the sole purpose of technical support.

5. How do we protect and safeguard your information?

We take appropriate technical and organisational measures to safeguard and protect your personal data from accidental or unlawful destruction, loss, alteration and unauthorised disclosure or access.

All personal data are stored in secure IT applications according to the EPO's security standards. Appropriate levels of access are granted individually only to the abovementioned recipients.

For systems hosted on EPO premises, the following basic security measures generally apply:

- User authentication and access control (e.g. role-based access control to the systems and network, principles of need-to-know and least privilege);
- Logical security hardening of systems, equipment and network;
- Physical protection: EPO access controls, additional access controls to datacentre, policies on locking offices;
- Transmission and input controls (e.g. audit logging, systems and network monitoring);
- Security incident response: 24/7 monitoring for incidents, on-call security expert.

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

For personal data processed on systems not hosted on EPO premises, the providers processing the personal data have committed in a binding agreement to comply with their data protection obligations under the applicable data protection legal frameworks. The EPO has also carried out a privacy and security risk assessment. These systems are required to have implemented appropriate technical and organisational measures such as: physical security measures, access and storage control measures, securing data at rest (e.g. by encryption); user, transmission and input control measures (e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), audit logging); conveyance control measures (e.g. securing data in transit by encryption)).

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

You have the right to access, rectify, and receive your personal data, to have your data erased and to restrict and object to the processing of your data, as outlined in Articles 18 to 24 of the EPO Data Protection Rules.

If you would like to exercise any of these rights, please write with details of your request to the delegated data controller at DPOexternalusers@epo.org. We will reply to your request without undue delay and in any event within one month of receipt of the request. However, Article 15(2) DPR

provides that this period may be extended by two further months where necessary in view of the complexity and number of requests received. We will inform you of any such delay.

In order to enable us to respond more promptly and precisely, you always need to provide certain preliminary information with your request. We therefore encourage you to fill in this form (for externals) and submit it with your request.

Please bear in mind that data protection is not an absolute right. It must always be balanced against other fundamental rights as well as freedoms and there may be circumstances where one or several data subject's rights may be refused to be granted.

The right of rectification can only apply to factual data processed in the framework of the investigative process. This means that only objective and factually inaccurate or incomplete data can be rectified, such as names, birth dates, addresses. In contrast, soft data, such as contained in subjective statements and interviews cannot be rectified. This does, however, not preclude you from complementing your statement with additional clarifications and comments.

Further, the above rights may be restricted for a temporary period of time on the legitimate grounds established by Article 25 of the Data Protection Rules and under Circular No. 420 Implementing Article 25 of the Data Protection Rules. The Circular provides that any such restriction will be limited in time, proportionate and will respect the essence of the data subject's rights.

Please also note that the data protection regulations do not foresee data subject rights for persons who are merely mentioned in evidence (such as complaint, witness and subject interviews and documentary evidence), but are not persons of interest to the investigative process.

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

Personal data is processed in accordance with Article 5a DPR.

Personal data is collected and processed in accordance with the following legal instruments, to ensure compliance with conduct obligations and accountability and preventing, detecting and addressing misconduct, Art. 21, 21a (1) Service Regulations, their Implementing Rules, Circular 341 and, Art. 20 Protocol on Privileges and Immunities.

8. How long do we keep your data?

Personal data will be kept only for the time needed to achieve the purposes for which it is processed and depending on the outcome of the investigative process.

After expiration of the applicable retention periods, all data will be irreversibly deleted.

The retention periods are:

- For allegations that are received but which are not considered to be with the IF remit – 12 calendar months from the date of receipt.
- For investigative processes that are closed at or prior to Preliminary Evaluation – 3 years from the date of closure.
- For investigative processes that are closed at the Investigation stage – 7 years from the date of closure.

9. Contact information

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

Review and legal redress

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