Data protection statement on the processing of personal data in the context of accident reporting at the EPO

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 refers to the processing of personal data in the context of accident reporting at the EPO.

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

Your personal data are processed in the context of accident reporting as follows:

Your personal data are processed in the context of accident reporting as follows:

1. The staff member suffering from an accident (called victim hereinafter) during his/her duties or in relation to his/her duties needs to fill out the accident registration form (ARF) via an online form provided in the EPO Intranet along with a detailed description of the accident's circumstances and some information on the health effects of the accident.
   In case of a visitor the form shall be filled out by the EPO contact person who invited the visitor.
   In case of a contractor the EPO contract manager fills out the form.
2. The ARF is submitted automatically via email to the EPO Health and Safety Service desk (Healthandsafety@epo.org) that forward it to the OSE (Occupational Safety Expert)
3. The OSE's register the accident on a database kept at the respective OSE's environment and initiates the investigation process, which looks only at the circumstances of the accident and does not disclose any personal information.
4. EPO Health Services, the EPO Occupational Health Physician and/or the respective OSE may get in touch with the victim to offer support.
5. The individual cases data is kept for 5 years to provide a record.
6. The ARF must be submitted by EPO staff within 10 days following the accident. In case the 'victim' is not in physical condition to complete the form the victim's line manager initiates the form. In case the visitor or the manager of the contractor cannot receive sufficient background information he/ she initiates the form with the available data within 24h following the accident. Detailed information is provided by the victim him/herself as soon as possible.

Data is handled by internal and external safety experts and safety assistants. These individuals have full access to the safety related records of the respective sites and process the information following the procedures in place.

The above-described processing operation is carried out for the following purposes:

- Promoting and ensuring the safety of EPO staff at the workplace.
- Improving the safety level within the Office.
- Improving emergency response.

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?

The following personal data of (a) employees and (b) contracting staff are processed:

- Contact details incl. phone numbers and working e-email address
- Age
- Gender
- Phone number
- Working email
- Employment information (e.g. job title, absences from work due to an occupational accident, existing disability or specific condition relevant for assessment of the accident)
- Medical data (e.g. type of injury in case of accident and information on first aid provided and/or hospitalisation)

3. Who is responsible for processing the data?

Personal data are processed under the responsibility of PD 4.4, 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 D Planning referred to in this statement.

External contractors involved in accident reporting may also process personal data, which can include accessing it.

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

The following recipients may have access to the data only on a need-to-know basis:

- EPO Health Services and Occupational Health Physicians – they support and cooperate with the Occupational Safety Expert when required

- PD 4.4 Operations offices (security) in case of an investigation

- Legal Services in litigation cases

Personal data may be disclosed to third-party service providers for e.g., maintenance and support purposes.

Personal data will only be shared with authorised persons responsible for the necessary processing operations. They will not be used for any other purposes or disclosed to any other recipients.

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

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

All personal data are stored in secure IT applications in accordance with the EPO's security standards. Appropriate levels of access are granted individually only to the above-mentioned recipients.

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

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

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

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

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

If you would like to exercise any of these rights, please write to the delegated data controller at dpl.pd44@epo.org . 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 or form (for internals) and submit it with your request.

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

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

Personal data are processed on the basis of Article 5(a) DPR:

- Processing is necessary for the performance of a task carried out in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning. Additionally, special categories of personal data (i.e. medical data) are processed based on Article 5(a) DPR in conjunction with Article 11(2)(f) DPR.

Personal data are processed on the basis of the following legal instrument:

Article 28 ServRegs - Assistance by the Organisation

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.

Accident Reports are stored in OpenText and kept for 5 years.

SAP-MyFIPS is used by the employees to submit via email their Accident Reporting Form. The emails generated in MyFIPS are deleted automatically after 3 months and for the accident report data stored in FIPS, the FIPS retention policy applies (currently permanently).

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 DPL_PD44@epo.org.

You can also contact our Data Protection Officer at dpo@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.