Data Protection Statement on the processing of personal data in the context of preventing access to the individuals that are banned to enter the EPO premises

Protecting your privacy is of the utmost importance to the European Patent Office (EPO). We are committed to respecting and protecting your personal data and ensuring your rights as a data subject. All data of a personal nature that identifies you directly or indirectly will be processed lawfully, fairly and with due care.

This processing operation is subject to the EPO Data Protection Rules (DPR).

The information in this communication is provided pursuant to Articles 16 and 17 of the DPR.

This statement refers to the processing of personal data related to the management of access to the EPO premises and more particularly the way the EPO security services prevent access to it to individuals for whom a ban to enter the EPO premises exists. This data protection statement explains the way in which the processing operation takes place.

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

Personal data are processed for the purpose of managing physical access to the EPO premises. The access control is used to monitor compliance with the existing provisions (House Rules and Security Circulars). The physical entrance controls are performed by an external security provider and is based on physical checks of access badges, identity documents and other legitimate forms of identification accepted by the Office in accordance with its House Rules (Circular 380).

To safeguard the safety and security of staff, visitors, confidential information and assets, access may be banned for individuals that are considered a threat for those ones or for investigative processes in which they may be part.

To achieve this purpose, Operations Office / Security Services manage a list of names from individuals that are banned to enter the premises. The list is used by external security contractors monitoring the accesses of individuals at entrances points of the buildings to verify that those are not on that list.

2. What personal data do we process?

The categories of personal data processed are the full name of the individual, its staff number in the case of those having a contractual relationship with the Office, start and end date of the prohibition to enter, department requesting the ban and contact person from that department.

3. Who is responsible for processing the data?

The processing of personal data is carried out under the responsibility of the DG4 - PD 44 - General Administration acting as the EPO's delegated data controller.

Personal data are processed by the EPO staff of Directorates Building Management involved in the management of this task.

External contractors from Directorates Building Management Security Services involved in this activity also process the personal data.

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

The personal data can be accessed on a need-to-know basis to the EPO staff working in DG4 - PD 44 - General Administration, Directorates Building Management.

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.

The data will only be accessed by other recipients (e.g., Ethics and Compliance, Police, Safety Expert) upon request and with permission of the Delegated Controller after consulting DPO for advice.

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, 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 above-mentioned recipients.

The following base 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 to lock offices
- Transmission and input controls (e.g., audit logging, systems and network monitoring)
- Security incidence response: 24/7 monitoring for incidents

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, receive your personal data, to request rectification, to request deletion -and to request restriction 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, external users should write to DPOexternalusers@epo.org, otherwise contact the delegated data controller at DPL.PD44@epo.org. 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) or this 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, according to Article 15(2) of the DPR, that period may be extended by two further months if necessary, taking into account 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 is processed in accordance with 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*' (Make sure the buildings are safe and secure).

Personal data is collected and processed in accordance with the following legal instrument:

The tasks attributed to the EPO (Circular 380, Art. 2. e): *Security staff will ensure compliance with these house rules, that the performance of the activities of the EPO is not obstructed and that the applicable rules and regulations are respected. They are authorised to give all orders and take all measures necessary for that purpose. In particular, they may carry out identity and security checks*.

The above reasons are considered as a targeted and proportionate way to achieve both, the safety of those coming to work, when security staff is responsible for the provision of the necessary emergency response, for keeping the adequate level of security of the information and assets at EPO.

8. How long can data be kept?

Personal data will be kept as long as the prohibition applies to the individual concerned. Personal data are deleted as soon as Physical Security is informed that the house has been lifted. In addition, a sanity check is performed by the so-called data manager at least once per year or whenever a change is reported to them.

In the event of a formal appeal/litigation, all data held at the time of the formal appeal/litigation shall be retained until the completion of its process.

9. Contact information

If you have any questions about the processing of your personal data, externals should contact the DPO and/or the delegated data controller at DPOexternalusers@epo.org. EPO employees should contact 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 data subject, you have the right to request review by the controller under Article 49 DPR and the right to seek legal redress under Article 50 DPR.