Data Protection Statement on the processing of personal data for the registration of presence of staff and contractors within the EPO premises outside office hours

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 registration of presence of staff and contractors within the EPO outside working hours. 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 is processed for the purpose of compliance with Circular 380 as well as to enhance the safety of staff and contractors coming to the office when emergency response teams normally available are not present.

As established under Circular 380, Art. 3.1.b and d, access and presence in the office is restricted to the opening hours of the buildings. Access to the office requires permission of D Building Management/Operations Office. Individuals coming to the Office outside working hours are requested to record their presence in the logbook kept by Security (Art. 3.1.d, Circular 380).

To comply with the above-established requirement, the security and reception staff at each site keep for staff and contractors an electronic logbook where they register the date of the visit, area/s being visited (office, rooms), office extension number or other contact number for emergency cases, full name, arrival and departure times and reason (work/private).

The data registered serves to enhance the situational awareness of the security teams present in the Office to provide emergency assistance in an effective way to those present in case this would be needed.

2. What personal data do we process?

The categories of personal data processed are as follows:

- Date of the visit
- Area/s being visited (office, rooms)
- Office extension or other contact number for emergency cases
- Full name
- Arrival and departure times
- Reason (work/private)
- If the visit was pre-announced or not. contractors are required to have pre-approval from their contract manager prior to the visit, not being allowed to come for private reasons outside office hours

3. Who is responsible for processing the data?

The processing of personal data is carried out under the responsibility of the DG4 - PD 4.4 - General Administration acting as the EPO's delegated data controller and represented by the D Building Management/Operations Office at each EPO site.

Personal data are processed by the EPO staff involved in the performance of this activity of the security services.

External security services contractors from D Building Management/Operations Office involved in this activity may also process, including access 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 4.4 - General Administration and when necessary to contract managers responsible for the administration of contractors. Staff and/or contractors who accessed the EPO premises outside the working hours and leave without informing the security staff will be contacted through email or phone. The purpose is to remind them about the importance to inform security for their own safety and for the safety of the security provider in charge of providing emergency assistance.

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

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 either on hard paper copies in a secure safe or in secure IT applications according to the EPO's security standards. Appropriate levels of access are granted individually only to the abovementioned recipients.

The following base security measures 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, on-call security expert.

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, 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, external users should write to DPOexternalusers@epo.org, otherwise contact 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 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, considering 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 under Article 5(a) DPR for the management and functioning of the EPO (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. 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, using for that purpose the necessary safety and security systems in a way that makes emergency response efficient.

8. How long can data be kept?

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

Personal data are deleted after 28 days.

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.