Data Protection Statement on the processing of personal data for the management of access control and management of access cards to the EPO

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 statement 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 control and access cards to the EPO. 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 access to the different EPO buildings and parking facilities in an efficient and effective way.

The card management system application is used to:

1. Manage access badges to provide access to buildings to EPO staff, family members, Council members, patent attorneys, contractors, EPO pensioners, service providers and visitors;
2. Verify that the visitors are not in the House Ban list and as such allowed to enter the EPO Premises before a visitor badge is assigned to them;

Verify the identity of the persons getting an EPO access badge by means of automated identity scanners, which at the same time also verify the authenticity of the identity document scanned.

In the access control system personal data are processed for the purpose of managing access to the different EPO buildings and parking facilities in an efficient and effective way.

The access control system is also used to monitor compliance with the existing provisions (House Rules and Security Circulars) as well as to:

1.- Provide access to EPO staff, visitors and contractors, including service providers, to EPO buildings;

2.- Register the access logs to areas where access has been granted to users;

3.- Register in an automated way (upon arrival of the vehicle to the entrance of the parking) the vehicle number plate of staff, contractors and visitors' vehicles having access to EPO premises to:

a) Monitor parking usage and limit the intervention of administrative staff for the registration of long-term parking requests.

b) Automate the way staff is informed whenever they violate the parking rules leaving their vehicles for longer terms than permitted (e.g., sending automated e-mails to staff not respecting the parking rules).

c) Manage in a more efficient way the available parking facilities (one vehicle per staff member).

To achieve No. 3, the number plates of the vehicles approaching the entrance of the parking are registered and linked to their access badge, this is done to identify the owner of the vehicle and to be able to monitor parking usage (one vehicle per person, one day maximum allowed parking time).

4.- Trigger alarms via Security Management System including door too long open alarms, forced opening of an entrance door or perimeter door and non-authorised badge used in an entrance.

2. What personal data do we process?

For the EPO staff, contractors' employees, EPO pensioners, Patent Attorneys and EPO Council members, the following categories of personal data are processed: Name, family name, badge number, building number, card validity, start and end of contract, phone number, access code, department, e-mail, employee group and subgroup, gender, badge number, language of communications, site, price list for discount, and technical details related to standard card management systems.

For visitors, the following personal data are processed: Name, family name, date of birth and/or identity document number and EPO contact person as well as the time stamps from their access to the buildings.

For EPO staff family members (FIPS registered partners and dependent children from EPO staff above the age of 16), personal data are processed to provide them a family badge to access the EPO sport facilities and semi-public areas if so, requested via MyFIPS interface by the sponsoring staff member. The badge will contain their picture, full name and ref. to the EPO staff member that is linked to the family member.

All data categories contained in a travel document (passport or national identity card) are processed but not stored. They are only processed during the identity verification done by means of identity document scanners being discarded once the result is presented.

Number plate of vehicles of staff and contactors having access to the EPO parking facilities as well as time stamps on when the building parking facilities were accessed. All data categories present in the Record of processing operation for the card management system (including staff and contractors' pictures for access control purposes).

Groups or individuals concerned:

- ✓ EPO staff
- ✓ EPO staff family members (above the age of sixteen)
- ✓ EPO pensioners
- ✓ Visitors (e.g Canteen users, External persons)
- ✓ Contractors' employees
- ✓ DPMA Berlin Office staff
- ✓ Patent Attorneys
- ✓ Council members

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 (Represented by the FM HoD at each EPO site) acting as the EPO's delegated data controller.

Personal data are processed by the EPO staff involved in the management of the respective initiative, project, activity of the Facility Management Security Services.

External contractors from Facility Management Security Services involved in this activity may also process, including access the personal data.

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

The personal data can be accessed on a need-to-know basis to the EPO staff working in DG4 - PD 44 - General Administration and when necessary to contract managers responsible for the administration of contractors.

Personal data might be disclosed to third-party service providers for maintenance or for support services.

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.

If other recipients (e.g. D. 0.4.4 Ethics and Compliance, Police, Safety Expert) request the information this will be individually asked to the Delegated Controller 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.

At least 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, on-call security expert.

Access to the data stored in the access control logs is limited to the administrators of the application. The data will only be accessed upon request and with the permission from the Controller after having obtained favourable advise from the DPO, except in extreme urgency cases in which DPO will be informed. Other users with access to the data such as the external security contractor will only have access to the data stored for the purposes of registering access to the EPO premises.

Access to the application and the data stored on it is limited to those with a need to know. Administrators from EPO Security have access to stored log files to monitor compliance and the external security contractor has limited access to operate the application.

Access to the application requires the authentication via BIT tools (password/active directory) plus an additional password for the application. For personal data processed by the external providers, such companies have committed in a binding agreement to comply with their data protection obligations under the applicable data protection legal frameworks.

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. 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): '*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, using for that purpose the necessary safety and security systems in a way that makes emergency response efficient.

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.

For the access control system (ACS), access logs older than 12 months will be overwritten by an automated routine programmed in the software.

Visitor data will only be kept for 28 days in line with the video surveillance records and for security purposes. This will allow physical security to proceed supporting investigations involving visitors access if criminal offences are reported.

For the card management system (CMS) data coming from FIPS will be stored and deleted following the retention times established by FIPS (an employee or contractor user data will be deleted upon deletion in FIPS).

For groups such as the Administrative Council or Patent Attorneys added manually by the so-called data manager, this one will perform, at least once per year or whenever a change is reported to them, a sanity check. During this check the data manager will verify if the data is still valid and correct, performing any necessary changes and/or deletions to keep the data up to date.

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 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.