EUROPEAN COMMISSION

PROTECTION OF YOUR PERSONAL DATA

This privacy statement provides information about the processing and the protection of your personal data.

Processing operation: Commission Physical Access Control System (PACS)

Data Controller: European Commission's DG HR and Security / Directorate Security / DS.3 Technical Security Unit

Record reference: DPR-EC-00655

Table of Contents

1. Introduction

The information in relation to processing operation "Commission Physical Access Control System (PACS)" undertaken by DG HR & Security is presented below.

The European Commission (hereafter 'the Commission') is committed to protect your personal data and to respect your privacy. The Commission collects and further processes personal data pursuant to Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data (repealing Regulation (EC) No 45/2001).

This privacy statement explains the reason for the processing of your personal data, the way we collect, handle and ensure protection of all personal data provided, how that information is used and what rights you have in relation to your personal data. It also specifies the contact details of the responsible Data Controller with whom you may exercise your rights, the Data Protection Officer and the European Data Protection Supervisor.

Physical Access Control within the Commission is ensured by the PACS system, implementing the security procedures and policies and producing access rights badges for individuals with a need to access European Commission buildings in Belgium and Luxembourg. Such persons mainly include Commission Statutory Staff (including permanent staff, contract and temporary agents), Seconded National Experts, Commission trainees, Commission contractors, staff of EU agencies, accredited journalists and other members of the press, staff family members and visitors.

2. Why and how do we process your personal data?

DG HR and Security collects and uses your personal information to ensure:

1. Security and protection of persons present inside Commission premises,
2. Secure access control and protection of Commission premises, information and assets,
3. Compliance with safety requirements – knowledge of the most accurate number of persons still present inside premises is required for evacuation and other emergency situations,
4. Compliance with legal requirements – the prevention, investigation, detection and prosecution of disciplinary or administrative infractions or criminal offences (processing is strictly based on data collection and subsequent handover of such data to the competent Commission bodies).

The system aims at the implementation of unique and coherent physical access controls throughout the Commission by performing all the required physical security functions. This includes physical access control automation and a uniform enforcement of procedures and security policies.

Processing done by the system is performed by a range of Information Systems and applications to produce access passes, control building access, monitor variations of noise levels and for video surveillance purposes following security alerts.

If the data subject needs access to specific zones protected by biometric devices, fingerprints may be encoded and stored on their personal access pass, which remains with the pass holder. The person concerned may decide, whether they want to use this specific access method or opt for an alternative method in these special cases.

3. On what legal ground(s) do we process your personal data

The processing operations of personal data are carried out under Article 5.1 of Regulation (EU) 2018/1725, **lawfulness of processing**:

> *"Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body."*

The basis for the processing referred to in points (a) of Article 5(1)(a) of Regulation (EU) 2018/1725 has been laid down in:

- Article 8 of Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission,
- Commission Decision (EU, Euratom) 2016/883 of 31 May 2016 on implementing rules for standard security measures, alert states and management of crisis situations in the Commission pursuant to Article 21 of Decision (EU, Euratom) 2015/443 on security in the Commission,
- Article 24 of the Staff Regulations of officials and the Conditions of Employment of other servants of the European Union.

As regards the voluntary use of fingerprint data stored on an access badge, the legal basis for processing is Article 5(1)(d) of Regulation (EU) 2018/1725, i.e. where the data subject has given consent to the processing of his or her personal data for one or more specific purposes.

Data collected may be used in the context of investigations led by the Security Directorate on its own initiative or at the request of IDOC or OLAF (see notifications DPR-EC-676 and DPR-EC-677) after agreement of the Director General of DG HR and Security.

4. Which personal data do we collect and further process*?*

Personal data are collected and further processed for anyone entering the Commission premises. This may include

- Commission Statutory staff
- Seconded National Experts
- Commission trainees
- Commission contractors
- Staff of other EU Institutions and agencies
- Staff family members
- Holders of Commission laissez-passer badges
- Visitors

and may consist of: full name, date of birth, photograph, nationality, gender, link with the Commission, current working status, place of visit, access period, telephone number(s), car plate number, e-mail, fingerprint minutiae (where appropriate), identity document number and dates, access rights, specific data related with roles within the Commission (including press, diplomatic representation), access point traversal information – badge number, date, time, direction, alarms and video captures if any. Not all data fields are necessarily processed or retained for each data subject. Fields processed or recorded are directly related to the kind of link the data subject has with the Commission or the reason for presence.

5. How long do we keep your personal data?

DG HR & Security only keeps your personal data for the time necessary to fulfil the purpose of collection or further processing, plus a reasonable retention period thereafter on condition that no contentious issues occurred; in this case, data will be kept until the end of the last possible

legal procedure. Thus, data are stored until termination of the link between the data subject and the Commission plus 6 months (e.g.: statutory staff: end of service / contract plus 6 months, external contractors: end of placement plus 6 months, visitor: end of visit plus 6 months, etc). Fingerprints, that have voluntarily been stored on badges, will remain on the badge for as long as it is being used by the data subject, i.e. normally 5 years.

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

In order to protect your personal data, the Commission has put in place a number of technical and organisational measures. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into consideration the risk presented by the processing and the nature of the personal data being processed. They ensure trusted telecommunications channels are used – Commission internal and external networks, dedicated lines to deployed security equipment. Security equipment is installed on a segregated or dedicated sub-network.

Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purposes of this processing operation.

All personal data in electronic format (e-mails, documents, databases, uploaded batches of data, etc.) are stored on the servers of the European Commission, which are located in secure zones. All processing operations are carried out pursuant to the Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission.

The Commission's contractors are bound by a specific contractual clause for any processing operations of your data on behalf of the Commission, and by the confidentiality obligations deriving from the transposition of the General Data Protection Regulation in the EU Member States ('GDPR' Regulation (EU) 2016/679).

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

Your personal data may be provided to the Commission staff responsible for producing Commission access passes, Commission staff and subcontractors under framework contracts with the Commission responsible for security management and monitoring, and Commission staff responsible for carrying out investigations as explained in notifications DPR-EC-00676 and DRP-EC-00677.

Your personal data may be shared with other EU Institutions, agencies or bodies for a specific purpose, such as car park access, mutual recognition of badging or for barring needs.

Interactive access to system processed data is restricted based on approved needs – i.e.: equivalent to need-to-know principle – and limited to the data associated with the user population under the responsibility of the operator or user – e.g.: Local Security Officer (LSO) for granting access to secure zones in their DG.

8. What are your rights and how can you exercise them?

You have specific rights as a 'data subject' under Chapter III (Articles 14-25) of Regulation (EU) 2018/1725, in particular the right to access, rectify or erase your personal data and the right to restrict the processing of your personal data. Where applicable, you also have the right to object to the processing.

You can exercise your rights by contacting the Data Controller, or in case of conflict the Data Protection Officer. If necessary, you can also address the European Data Protection Supervisor. Their contact information is given under Heading 9 below.

Where you wish to exercise your rights in the context of one or several specific processing operations, please provide their description (i.e. their Record reference(s) as specified under Heading 10 below) in your request.

9. Contact information

- **The Data Controller**

If you would like to exercise your rights under Regulation (EU) 2018/1725, or if you have comments, questions or concerns, or if you would like to submit a complaint regarding the collection and use of your personal data, please feel free to contact the Data Controller: EC-SECURITY-PACS@ec.europa.eu

- **The Data Protection Officer (DPO) of the Commission**

You may contact the Data Protection Officer (DATA-PROTECTION-OFFICER@ec.europa.eu) with regard to issues related to the processing of your personal data under Regulation (EU) 2018/1725.

- **The European Data Protection Supervisor (EDPS)**

You have the right to have recourse (i.e. you can lodge a complaint) to the European Data Protection Supervisor (edps@edps.europa.eu) if you consider that your rights under Regulation (EU) 2018/1725 have been infringed as a result of the processing of your personal data by the Data Controller.

10. Where to find more detailed information?

The Commission Data Protection Officer (DPO) publishes the register of all processing operations on personal data by the Commission, which have been documented and notified to him. You may access the register via the following link: http://ec.europa.eu/dpo-register.

This specific processing operation has been included in the DPO's public register with the following Record reference: DPR-EC-00655.