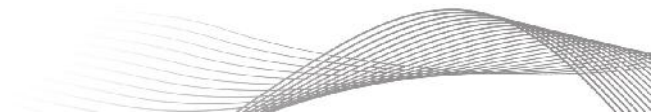


EDPS record of processing activity

Record of EDPS activities processing personal data, based on Article 31 of 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, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

Nr.	Item	Description
Access to building and parking policy for staff		
1.	Last update of this record	03/12/2018
2.	Reference number	34
3.	Name and contact details of controller	<p>European Data Protection Supervisor (EDPS) Postal address: Rue Wiertz 60, B-1047 Brussels Office address: Rue Montoyer 30, B-1000 Brussels Telephone: +32 2 283 19 00 Email: edps@edps.europa.eu</p> <p>Responsible department or role: edps-lso@edps.europa.eu</p> <p>Contact form for enquiries on processing of personal data to be preferably used: https://edps.europa.eu/node/759</p>
4.	Name and contact details of DPO	edps-dpo@edps.europa.eu
5.	Name and contact details of joint controller (where applicable)	<p>EP DG SAFE Directorate-General for Security and Safety Directorate for Proximity and Assistance, Security and Safety Security and Safety Brussels Unit BRU - WIB 01M087 - Tel. +32 228 46025</p>



Nr.	Item	Description
		safe.EDS2@europarl.europa.eu ;
6.	Name and contact details of processor (where applicable)	-
7.	Short description and purpose of the processing	<p>The EDPS is located in premises belonging to the European Parliament (EP). The EP manages, among others, the control of access to their buildings.</p> <p>Based on a Cooperation Agreement, the EP performs access control also on EDPS' behalf to protect both EP and EDPS' assets.</p> <p>The purpose of the Access Control System is to protect the European Data Protection Supervisor premises against unauthorised access and against both external and internal threats. It is essentially composed of end point technical components (card readers connected to the badges used by staff members and alarm points) installed at the the sites entrances. Such installations use repositories where staff authorisations are stored and against which information in badges is matched in order to implement and enforce access controls.</p> <p>Only cars bearing an EP vignette and inserted in a special list can have access and are thus authorised to enter the parking in the EDPS building.</p> <p>According to the EP, independently of the technology used, no other information apart from the physical badge number is read from or stored on the badge.</p> <p>The access control system aims at providing:</p> <ul style="list-style-type: none"> • Security measures to protect the persons and premises of the site. • Authorisation of access to site (registration of staff, visitors and vehicles), • Physical protection of the site (guards, alarms, video surveillance, etc.) • Protection of organisational assets, information and monitoring of information system



Nr.	Item	Description
		<p>security.</p> <p>The transfer of personal data from the EDPS to the European Parliament is necessary in order to validate the access authorizations and to activate the transponders allowing access to the premises of the EDPS.</p>
8.	Description of categories of persons whose data the EDPS processes and list of data categories	<p>All staff members of the EDPS: officials, contractual agents, external contractors, interim agents and trainees.</p> <p>The data at stake are the following:</p> <ul style="list-style-type: none"> - Identification data (surname, first name, date of birth, nationality, administrative address, staff number, office telephone number) - Date of recruitment and type of contract - Family data (only for staff requesting family accreditation and when a family access badge is issued) - Type of access authorization (type of Parliament buildings, limited access during the weekend, etc.) - Car data (only for staff requesting access to the car park of the building) <p>The personal information is provided by the Human Resources Unit. The information concerning the family and personal car are provided by the EDPS officials when introducing the request.</p>
9.	Time limit for keeping the data	<p>Personal data will be kept as long as the staff member is covered by a valid access authorisation. As soon as a staff member leaves the EDPS, all his/her personal data will be removed from the list given to the EP services. For security reasons EP DG SAFE will keep the data for one year after the staff member departure and then it will delete them.</p>



Nr.	Item	Description
10.	Recipients of the data	Only Security services (agents) of the European Parliament and EDPS Local Security Officer (LSO)
11.	Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?	No such transfers.
12.	General description of security measures, where possible.	In order to safeguard personal data against any possible misuse or unauthorised access, electronic information are accessible with a restricted access for the recipients only and the Local Security Officer of the EDPS (habilitation d'accès, password and back-up). For paper copies of the lists they should be protected by keeping them locked away when not in use and stored in a locker, thrower or cupboard .
13.	For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the data protection notice:	Please refer to the Access to building for staff data protection notice. The EDPS LSO will regularly (at least once per year) request staff members to update their data.

