

EDPS Record of Processing Activity

Nr.	Item	Description
		Access to EDPS building by visitors
	Last update of this record	5/05/2025
2.	Reference number	38
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>Delegated controller: HRBA unit (edps-building@edps.europa.eu) Contact form for enquiries on processing of personal data to be preferably used: https://www.edps.europa.eu/about-edps/contact_en</p> <p>Separate controller: European Parliament EP DG SAFE Directorate-General for Security and Safety Directorate for Safety, Access and Assistance - Access and Visitors Unit SAFE.AccesSecuriteBxl@europarl.europa.eu For more information, please refer to the:</p>

Document info

Roles & Contact Details

		<ul style="list-style-type: none"> • EP record • EP data protection notice <p>Contact for enquiries: EP DPO ; data-protection@europarl.europa.eu</p>
4.	Name and contact details of DPO	dpo@edps.europa.eu
5.	Name and contact details of joint controller (where applicable)	
6.	Name and contact details of processor (where applicable)	
7.	Short description and purpose of the processing	<p>The EDPS (MTS) building 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 against unauthorised access and any security threats.</p> <p>The purpose of the Access Control System is to protect the EDPS premises against unauthorised access and against security threats.</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 (controlling and, if applicable, granting) of access to site (registration of visitors and vehicles); • Physical protection of the site (guards, alarms, video surveillance, etc.);

Roles & Contact Details

Description of processing

		<ul style="list-style-type: none"> • Protection of organisational assets, information and monitoring of information system; • Investigating security incidents; • Evaluating threats and analysing risks. <p>Accreditation of visitors</p> <p>Accreditation of visitors V-PASS is used to manage the accreditation of visitors entering the Parliament’s premises in the context of both personal visits and group visits or an events.</p> <p>Staff members who host a visit or an event have to create an entry in V-PASS and then add their visitors and the required data (all EDPS staff have a V-PASS account, except external staff and trainees). There might also be cases where staff members who host a visit or event adds names and email addresses, and then the visitors complete their own data in the vpass. Or, alternatively, there might be cases (such as individual visitors, private visits, small last-minute meetings) where visitors’ personal data will be asked in advance.</p> <p>Link to V-PASS: https://accreditation.europarl.europa.eu/europarl/epvisitors/</p>
8.	Description of categories of persons whose personal data is processed and list of data categories	<p>Personal data of visitors who would like to have access to EDPS building will be processed.</p> <p>Registration of individual visitors</p> <p>EDPS staff can request an accreditation for individual visitors or groups to DG SAFE’s Access and Visitor Unit, via the V-PASS application.</p> <p>Data processed as part of visitor registration in V-PASS:</p> <ul style="list-style-type: none"> • date of visit (start and end date)

Description of processing

	<ul style="list-style-type: none"> • first name(s) • last name(s) • date of birth • nationality • document type (ID card or passport) • document number • document expiry date • type of visit (private or professional) • (optional) organisation • email address <p>Visitors data are gathered by EDPS:</p> <ul style="list-style-type: none"> • by email • via a dedicated registration form on EDPS Website <p>The staff member responsible for the visit/event has to add the visitors in VPASS providing at that stage at least first name, last name and email address. The visitor will receive an email with a link to his/her profile in VPASS in order to provide all the other required data as listed above.</p> <p>Alternatively, visitors' information can be imported in bulk (i.e. from an xls table).</p> <p>Personal data of visitors registered in V-PASS is transmitted to DG SAFE's internal database (iPACS) where a verification is performed about whether there is a restriction on access on the visitor concerned. The result of this verification is sent back to the visitor registration tool (V-PASS). A nominative access badge will be provided to each visitor.</p>	Description of processing
--	--	---------------------------

	<p>Badge collection takes place at an interactive kiosk placed at visitor entrances. At the kiosks, visitors scan their identity document (ID card or passport) where the below-mentioned data are extracted by the MRZ of kiosk:</p> <ul style="list-style-type: none"> • first and last name • date of birth • nationality • ID document type • ID document number • ID document expiry date <p>The ID document will be recognised only if it is the same one that was used for vpass registration.</p> <p>Visitors must carry their identity documents and access badges and always be accompanied by an EDPS staff member or by a security agent when moving around the EDPS building.</p> <p>Some other personal data may be collected in order to grant access to the EDPS premises. For example, agents may record the entry to, and exit from the building of visitors and vehicles (as well outside the normal opening times).</p> <p>Agents may conduct other necessary operations related to access control.</p> <p>In addition, when badges are printed (either at an accreditation desk or through a kiosk) visitors' personal data is sent to DG SAFE's internal database (iPACS) whereas verification is performed about whether there is a restriction on access on the visitor concerned. The result of this verification is sent back to the visitor registration tool (V-PASS).</p>	<p>Description of processing</p>
--	--	----------------------------------

		<p>Vehicles:</p> <p>Pass holders entitled to enter the parking, might send a request to the Access and visitors Unit with further personal data regarding their vehicle and the person entitled to use it.</p> <p>In order to issue a car pass, the following personal data is processed:</p> <ul style="list-style-type: none"> • email • plate number • country of registration • fuel type • make • type • colour and • RFID tag number <p>For service providers wishing to enter the parking, the following additional information should be provided:</p> <ul style="list-style-type: none"> • name external company (firm) • name and first name of the responsible official and • contract number • pre-approval of management of inventoried assets of the building 	Description of processing
9.	Time limit for keeping the data	<p>There are different retention periods depending on the categories of personal data:</p> <ul style="list-style-type: none"> • Visitor's personal accreditation data (first and last name, date of birth, nationality, ID document type and number, ID document expiry date, (optionally) organisation/employer) is stored for one year. 	Retention

		<ul style="list-style-type: none"> Personal data relating to the access's history (extract from badges use at the entrances to EP premises) is kept for 4 months. 	
10.	Recipients of the data	<p>DG SAFE may transmit data to the following:</p> <ul style="list-style-type: none"> other DGs of the EP the President and the Secretary General of the EP <p>Within the framework of investigations, accreditation data can be transmitted to other recipients (i.e. national authorities of the Member States). This is covered under the EP Record number 18: 'Enquêtes de sécurité et investigations complémentaires'.</p>	Recipients
11.	Are there any transfers of personal data to third countries or to international organisations? If so, to which ones and with which safeguards?	No such transfers occur.	Transfers
12.	General description of security measures, where possible.	The security measures applicable to V-PASS web-applications (i.e. information security measures, access rights based on need-to-know).	Security
13.	For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the data protection notice:	https://www.edps.europa.eu/data-protection/our-work/publications/other-documents/2025-05-05-data-protection-notice-access-edps-building-visitors_en	Data Protection Notice