

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
		Communication to staff on security alerts
1.	Last update of this record	10.10.2023
2.	Reference number	75
3.	Name and contact details of controller	<p>1. 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: Local Security Officer (LSO) 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> <p>The EDPS will use both the European Commission (EC)'s and the European Parliament (EP)'s crisis communication systems.</p> <p>For consent collection, EDPS will use EUSurvey. In this context, The EDPS is responsible for the parameterisation and content of EUSurvey and for the processing of personal data within the survey (see EDPS record).</p>

Nr.	Item	Description
		<p>2. The EC is separate controller for its security alerting system - EUWARN ('the EC system')</p> <p>European Commission Human Resources and Security (HR), DS.1 unit</p> <p>See record: DPR-EC-00826.5 and the dedicated intranet page for EUWARN.</p> <p>3. The EP is separate controller for its SMS crisis communication system ('the EP system')</p> <p>EP Directorate General for Security and Safety Directorate for Safety, Access and Assistance Emergency and Control Room Unit</p> <p>EP Parliament's Secretariat Directorate for Innovation and Central Services Risk, Crisis and Business Continuity Unit</p> <p>Risk-Crisis-BusinessContinuity@europarl.europa.eu</p> <p>See the data protection notice and the record.</p> <p>4. The EC is a separate controller for the EU Login system, which is used for logging in the EUSurvey designed to collect staff consent for the EP system. See applicable record: DPR-EC-03187.1</p>
4.	Name and contact details of DPO	dpo@edps.europa.eu



Nr.	Item	Description
5.	Name and contact details of joint controller (where applicable)	
6.	Name and contact details of processor (where applicable)	<p>The EC system</p> <ul style="list-style-type: none"> - Personal data of security notification recipients are stored in the COMREF database managed by DG DIGIT under the authority of DG HR. - EUWARN, as contractor <p>The EP system</p> <ul style="list-style-type: none"> - The EP uploads the phone numbers in the external SMS web-interface application managed by the Ring Ring Company NV. <p>EUSurvey</p> <p>For consent collection, EDPS will use EUSurvey.</p> <ul style="list-style-type: none"> - The EC-DIGIT is the processor for the web-based interface of the survey and the hosting of survey data and any submitted responses. <p>For more information, see the DPR-EC-01488.1 and the data protection notice. Contact: DIGIT-DATA-PROTECTION-COORDINATOR@ec.europa.eu</p>
7.	Short description and purpose of the processing	<p>The aim of this processing activity is to ensure that, in the event of a crisis, the EDPS staff will receive SMS crisis communications either from the EC or the EP or both.</p> <p>The EC EUWARN system is used to inform staff of incidents (e.g. demonstrations, evacuations or police interventions inside or close to EC buildings) and emergencies and advises them on what to do.</p>



Nr.	Item	Description
		<p>EDPS staff will receive via EUWARN e-mails to their professional email address - this is an automated process, so staff do not need to enroll.</p> <p>SMS alerts will only be sent to private phone number of staff based on their enrolment in the system. HR.DS1.002 informs staff members timely about a nearby security incident and instructs them on how to stay safe. To do so, HR.DS1.002 selects in its security communication tools the affected building as target audience of a security notification.</p>
8.	Description of categories of persons whose data the EDPS processes and list of data categories	<p><u>Categories of persons</u></p> <p>EDPS staff</p> <p><u>Categories of personal data</u></p> <p>For the EP system</p> <ul style="list-style-type: none"> - surname, first name - private mobile telephone number <p>The collected updated information will be provided to the EP by the LSO on a monthly basis.</p> <p>For the EC system</p> <ul style="list-style-type: none"> - first and last name - professional email address - professional mobile phone number - private mobile phone number if authorised beforehand by the subject - administrative residence (building, floor, office number) - administrative service



Nr.	Item	Description
		<p>Personal data processing in the context of security incidents is carried out by Commission staff members holding a valid security clearance on level SECRET UE / EU SECRET and authorised to send security notifications. Access to relevant security communication tools is granted on a need-to-access basis and subject to user authentication and specific access rights.</p>
9.	Time limit for keeping the data	<p>For the EP system</p> <p>Personal data will only be stored by the LSO for the time that the data subject voluntarily enrolls in the system and for as long as he/she is in the EDPS' service. The LSO updates the file on a monthly basis.</p> <p>Data of staff who have been provided with a mobile telephone for professional use will be stored for as long as the telephone in question is in use by the data subject.</p> <p>For the EC system</p> <p>In accordance with the EC DPR-EC-00826.5,</p> <p>- the following categories:</p> <p><i>'First and last name; professional email address; professional mobile phone number; administrative residence (building, floor, office number); administrative service (retrieved from COMREF)'</i></p> <p>are processed <i>'for as long as the subject works at the' [EDPS] 'plus maximum three months. In case of e.g. a complaint by the subject, the three months period is necessary to allow Commission security services to verify whether a subject has indeed been warned of a security incident.'</i></p> <p>- the following category:</p> <p>private mobile number</p> <p><i>'For as long as the subject authorises the Commission to process their private contact data plus maximum three months. In case of e.g. a complaint by the subject, the three months period is</i></p>



Nr.	Item	Description
		<i>necessary to allow Commission security services to verify whether a subject has indeed been warned of a security incident.’</i>
10.	Recipients of the data	<p>For the EP system</p> <ul style="list-style-type: none"> - The service in charge in EP (see above) - The EP uploads the phone numbers in the external SMS web-interface application managed by the Ring Ring Company NV. <p>For the EC system</p> <ul style="list-style-type: none"> - HR.DS1.002 staff in charge of communicating on security incidents - EUWARN contractor in charge of operating and maintaining the EUWARN system; the contractor’s access is covered by an appropriate security convention authorised and signed by DG HR
11.	Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?	No.
12.	General description of security measures, where possible.	<p>For the EP system</p> <p>The excel file containing staff’s personal data will be held in a restricted share drive by the LSO. Montly sending to the EP will be done in an encrypted mode.</p> <p>For the EC system</p> <p>According to EC DPR-EC-00826.5,</p> <p><i>‘All personal data in electronic format (e-mails, documents, databases, uploaded batches of data, etc.) are stored either on the servers of the European Commission or of its contractors. All processing operations are carried out pursuant to the Commission Decision (EU, Euratom)</i></p>



Nr.	Item	Description
		<i>2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission.'</i>
13.	For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the data protection notice:	Data protection notice published internally.

