

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
		Business Continuity Plan
1.	Last update of this record	6.10.2023
2.	Reference number	33
3.	Name and contact details of controller	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 Responsible department or role: edps-lso@edps.europa.eu Contact form for enquiries on processing of personal data to be preferably used: https://edps.europa.eu/node/759
4.	Name and contact details of DPO	dpo@edps.europa.eu
5.	Name and contact details of joint controller (where applicable)	N/A
6.	Name and contact details of processor (where applicable)	-

Nr.	Item	Description
7.	Short description and purpose of the processing	<p>The Business Continuity Plan (BCP) is a plan to deal with possible business continuity incidents affecting EDPS' functions. Its aim is to ensure that the institution is able to continue operation to the extent possible whatever the nature of a major disruption. The purpose of the BCP and the associated Guidance is to provide the EDPS with a structured approach and guidance to Business Continuity (BC), as EDPS needs to plan and prepare for unforeseen disruptions to its activities.</p> <p>The BCP is in place to ensure that the institution is able to continue operation to the extent possible whatever the nature of a major disruption.</p> <p>The purpose of the processing is to enable the institution, in the context of a BCP, to contact each EDPS staff member where necessary. All personal data submitted will be used for the sole and exclusive purpose of informing staff in case of BCP action.</p>
8.	Description of categories of persons whose data the EDPS processes and list of data categories	<p>All staff members of the EDPS.</p> <p>The personal data that are gathered during the processing operations are the following:</p> <ul style="list-style-type: none"> • Name and surname • The list of professional phone numbers with professionals e-mails and location rooms • Personal mobile phone numbers • The personal data contained in the BCP document (names of document reviewers, and names of contacts of the European Parliament BC) as well as the EP BCP document (see also section 10). <p>Private phone numbers are stored in the emergency phone, kept by the LSO/BCP Desk Officer and used only in cases of concrete emergencies causing a work disruption. When printed out they will be put in two sealed envelopes (entrusted to the Secretary-General and the BC Desk officer), and in an Excel file on an encrypted USB stick to be locked away.</p> <p>The Secretary-General and Heads of Units/Sectors can send e-mails with information to staff using staff professional e-mail addresses.</p>



Nr.	Item	Description
		<p>Staff with questions can contact the Heads of Units/Sectors on their work phone in this context.</p> <p>All staff are equipped with professional laptops and, as such, it is always possible to consult professional emails in case the incident has not affected internet communications.</p>
9.	Time limit for keeping the data	<p>Personal data will be kept as long as the staff member is a member of the EDPS. As soon as a staff member leaves the EDPS, all his/her personal data will immediately be removed from the phone lists both in the emergency EDPS mobile phone and in the 2 sealed envelopes.</p>
10.	Recipients of the data	<p>The BCP, with the contact details of the key business continuity actors, is sent also to the European Parliament security services as the EDPS building belongs to the EP. The BCP relies only on having a permanent and reliable contact with the security services of the Parliament. The reverse scenario, where we receive the BCP of the EP with their key actors' contact details, should also be taken into account where it is the Duty officer who informed EP security on an incident which will trigger measures from EP side.</p> <p>Personal mobile phones data will never be disclosed to any third parties.</p>
11.	Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?	<p>No such transfers.</p>
12.	General description of security measures, where possible.	<p>In order to safeguard personal data against any possible misuse or unauthorised access, electronic and paper information is accessible with a restricted access only (possible use of password for excel files to be held in secure hard drives and sealed envelopes for paper files), and only to people having a need to know.</p>
13.	For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the data protection notice:	<p>Please refer to the BCP data protection notice, which is published on the EDPS intranet. The EDPS will regularly (at least once per year) request staff members to update their data.</p>



