Eurojust record of processing activity

Record of processing personal data activity, 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

Part I –Article 31 Record (this part is publicly available)

Nr.	Item	Description
Incident Management system		
1.	**Last update of this record**	
2.	**Reference number** [For tracking, please contact the DP Office for obtaining a reference number.]	SU-06 (MARCH 2020)
3.	**Name and contact details of controller** [Use functional mailboxes, not personal ones, as far as possible - this saves time when updating records and contributes to business continuity.]	Head of Security Unit Security@eurojust.europa.eu
4.	**Name and contact details of DPO**	dpo@eurojust.europa.eu
5.	**Name and contact details of joint controller (where applicable)** [If you are jointly responsible with another EUI or another organisation, please indicate so here (e.g. two EUIs with shared medical service). If this is the case, make sure to mention in the description who is in charge of what and whom people can address for their queries.]	Not applicable
6.	**Name and contact details of processor (where applicable)**	The system is managed by duly authorized members of the Security Management Sector (Security Unit) and duly

Nr.	Item	Description
	[If you use a processor (contractor) to process personal data on your behalf, please indicate so (e.g. 360° evaluations, outsourced IT services or pre-employment medical checks).]	authorized outsourced security guards operating the Security Control Room (SCR), hereinafter the security services at Eurojust.
7.	**Purpose of the processing** [Very concise description of what you intend to achieve; if you do this on a specific legal basis, mention it as well (e.g. staff regulations for selection procedures).]	The purpose of the processing of personal data in the Incident Management System is to record the incidents at and malfunctions or damages to Eurojust premises and systems detected by the security services at Eurojust; and to report such incidents, malfunctions or damages to the relevant entities at Eurojust. Use of personal data is restricted to the bare minimum, using as much as possible call signs or functions.
8.	**Description of categories of persons whose data are processed and list of data categories** [In case data categories differ between different categories of persons, please explain as well.]	The system may process data from any person present at Eurojust involved in a security or safety incident or a damage to the premises or assets. The data categories processed are: • First Name • Last Name • License plates
9.	**Time limit for keeping the data** [Indicate your administrative retention period including its starting point; differentiate between categories of persons or data where needed (e.g. in selection procedures: candidates who made it onto the reserve list vs. those who did not).]	The system will retain data for 6 months. The data will be deleted automatically by the system after the retention period.
10.	**Recipients of the data** [Who will have access to the data within Eurojust? Who outside Eurojust will have access? Note: no need to mention entities that may have access in the course of a particular investigation (e.g. OLAF, EO, EDPS).]	Maintenance of the system is performed by duly authorized officers in the IM Unit.

Nr.	Item	Description
11.	**Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?** [E.g. processor in a third country using standard contractual clauses, a third-country public authority you cooperate with based on a treaty. If needed, consult DPO for more information on how to ensure safeguards.]	No
12.	**General description of security measures, where possible.** [Include a general description of your security measures that you could also provide to the public.]	The system is segregated from the rest of the building and Eurojust ICT infrastructure. It is placed in a standalone ICT network, which is not connected to the Internet or any other internal network. It may send emails to notify incidences but not receive them. The data processing capabilities are installed in specially protected areas. Access to such areas is given only to duly authorized personnel.
13.	**For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the data protection notice:** [While publishing the data protection notice is not strictly speaking part of the record, doing so increases transparency and adds no administrative burden, since it already exists.]	*Data protection notice (could be a hyperlink or a file attached to this record)*