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
Daily list of presence in the building		
1.	**Last update of this record**	
2.	**Reference number** [For tracking, please contact the DP Office for obtaining a reference number.]	SU-07 (March 2021)
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)**	Duly authorized Security Officers of the Security Management Sector and duly authorized outsourced security guards

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).]	operating the Security Control Room (SCR) collect the data in a list, submitted daily to the Head of the Security Management Sector and the Head of Security Unit. After the data are collected, only Head of the Security Management Sector and the Head of Security Unit can store and access the data.
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).]	• Due to the COVID-19 pandemic, for safety and security reasons SEC needs to know instantly who is in the building at any time, so that in case of an emergency we can ensure proper assistance and, if necessary, complete evacuation. • In case the agency identifies a person as infected with COVID-19 after she/he has had access to the building, Eurojust needs to know who may have been in contact with she/he to follow up with them. • iProtect is designed to work combining information from badges and from biometrics. The latter has been disabled recently for health prevention reasons, but we have not had the chance to test whether the system stills collects information properly with this new setting. We trust it is working, but we do not have 100% assurance. It is crucial for safety, security and health reasons that we ensure that information about who is/was and when in the building is available at all times during this COVID-19 pandemic. • iProtect stores data for 14 days. After that the system deletes it automatically. There is no scientific certainty about the exact incubation period of COVID-19. There is a 14 days standard quarantine period, but it may vary depending on the person. In the event of a person that has accessed the building being infected, the 14 days data retention period in iProtect is therefore insufficient to provide information to identify the persons she/he may have contacted within the building.
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 categories of data subjects are the following: • National Members, Deputies and Assistants; • The representative of Denmark at Eurojust; • Liaison Prosecutors of third States seconded at Eurojust on the basis of a cooperation agreement, their assistants and staff of their offices; • Eurojust staff members; • Seconded National Experts (SNEs); • interns;

Nr.	Item	Description
		• judges and prosecutors on a traineeship sponsored by the European Judicial Training Network (EJTN); and • Any other person performing a job at Eurojust established by means of a legal provision or a formal decision of the College of Eurojust; • Contractors working regularly at Eurojust being granted unescorted access to physically protected areas; • Cooperation partners i.e. post-holders of EU institutions, agencies and bodies using badges issued by Eurojust on the basis of an agreement (e.g. Europol, European Commission) The data categories processed are: • First Name • Last Name • Organisational Unit • Date and time of access. • Date and time of exit.
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 daily lists are kept for 30 days. Both lists are revised and deleted manually on a daily basis, also from the recycle bin.
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).]	None, the lists are not shared within the organisation.

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 lists are kept in a secure environment, with access strictly limited to the Head of the Security Management Sector and the Head of Security Unit. The lists are not shared or copied.
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)*