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
1.	**Last update of this record**	Building occupancy statistics
2.	**Reference number** [For tracking, please contact the DP Office for obtaining a reference number.]	**SU-08 (September 2022)**
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)** [If you use a processor	Only limited number of duly authorized Security Officers of the Security Management Sector and the Head of Security Unit (further - HoU or HoS) will be able to access and process

Nr.	Item	Description
	(contractor) to process personal data on your behalf, please indicate so (e.g. 360° evaluations, outsourced IT services or pre-employment medical checks).]	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).]	• Because of the COVID-19 pandemic, the Commission established a new, more flexible regime for teleworking. It would require that the use of the building (e.g. office space allocation) and the services provided to post holders and visitors (e.g. catering) would need to be optimised in view of this new situation. • In addition, the agency needs to keep a record of the people flow in the building for different administrative reasons (e.g. insurance) and to plan resources in relation to such flows. • Using entry data from iProtect system, the Security Unit prepares weekly occupancy statistics of post holders for Eurojust management. A real sample of such statistics below. Only one Officer directly tasked by the HoU or HoS will extract the data. The data will be only used by the HoU/HoS in order to produce the following statistics with no personal data:

Date	Number of people	Weekly average	Weekly occupancy rate
06-Jun	19		
07-Jun	270		
08-Jun	246	195.2	49% occupancy
09-Jun	239		
10-Jun	202		

Such measure is of a temporary nature and it will have to be assessed in January 2023 whether it is still necessary and proportionate taking into account the overall situation at that point in time. The data retrieved to produce the statistics (aggregated data) shall not and will not be used for any other purposes strictly respecting the purpose limitation principle enshrined in Article 4(1)(b) of Regulation 2018/1725. The data processing for statistical purpose will be processed in accordance with Article 13 of Regulation 2018/1725.

Nr.	Item	Description
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; • 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.
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).]	Personal data in iProtect is automatically deleted after 14 days. Same applies to daily visitors lists stored in DMS. The extracted data shall be used only for this specific purpose and deleted as soon as possible; and in any case not later than three days after the extraction. The statistics are kept in DMS without any specific expiry date because they do not contain any personal data.

Nr.	Item	Description
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).]	Administrative Director, Heads of Department, Head on ELU, Security Management Sector will receive only the aggregated statistics. The raw personal data shall not be shared outside the Security Unit.
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 with aggregated data are kept in a secure environment (DMS), with access strictly limited to the Security Management Sector and the Head of the Security Unit.
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*