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
iProtect system		
1.	**Last update of this record**	
2.	**Reference number** [For tracking, please contact the DP Office for obtaining a reference number.]	SU-03 (February 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)**	Duly authorised members of the Security Management Sector

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).]	have view and edit rights in iProtect. The duly authorised outsourced security guards operating the Security Control Room (SCR) have view access only to iProtect.
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 Security and Safety related systems protect Eurojust building and key Eurojust assets, i.e. persons working and visiting Eurojust, physical assets, and information. An AD Decision (pending adoption in March 2020) will establish an access management policy at Eurojust. The iProtect application partially implements this policy. It manages access through badges issued individually to persons working at Eurojust or having a special work relationship with the agency. It processes personal data for the following purposes: • Ensure that only authorized persons enter Eurojust premises and the specific security zones within. • Detect any attempt of an unauthorized person to enter security zones; • Keep a temporary record of access events to investigate potential security and safety incidents.
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.]	**iProtect** processes data from: • 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; • 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

Nr.	Item	Description
		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 • Photo • Biometric information (Palm vein template based on the right and left palms scan) • Validity of the badge (from - to date) • Organisational Unit • Access to the different Security Zones. The access badges contain the following information: • Printed on the badge: First name, Last Name, Photo and date of end of contract. • Stored on encrypted chip mounted on the badge: Unique Badge ID, access permission for off-line card readers.
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).]	iProtect retains the badge holders' data as long as they have a relationship with Eurojust. iProtect keeps records of access events for 14 days. The system automatically deletes the data after this 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.	The company responsible for technical maintenance of iProtect (Heijmans) has full access to the system and administrator rights, without actual access to personal data. Maintenance occurs following a four-eye principle whereby one Eurojust Security Officer has to be present during the operations.

Nr.	Item	Description
	OLAF, EO, EDPS).]	
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.]	iProtect 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.
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)*