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

2

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

Nr.	Item	Description
Security screening procedure		
1.	**Last update of this record**	2018
2.	**Reference number** [For tracking, please contact the DP Office for obtaining a reference number.]	SU-01 (January 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 Clearance@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 (contractor) to process personal data on your	Clearance and Register Officer

Nr.	Item	Description
	behalf, please indicate so (e.g. 360° evaluations, outsourced IT services or pre-employment medical checks).]	
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).]	Personal data is collected and further processed in order to implement the procedure provided in Administrative Director Decision on rules on security clearance of personnel, dated 18 June 2009.
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.]	First name, family name, nationality, date of birth and place of birth of post holders on sensitive posts (CA, TA, SNE to the Administration).
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).]	a) The retention period for the Personal Information Forms of active post holders on sensitive posts is from the moment the post holder provides the PIF to the Clearance Office until the initiation of a renewal procedure where a new PIF is produced; b) The retention period for the Personal Information Forms of departed post holders on sensitive posts is from the moment the post holder provides the PIF to the Clearance Office until the date of the departure of the post holder from Eurojust; c) The retention period for certificates/assurances for access to EU classified information is until their expiry date; d) The retention period for the Records documenting the security screening process is from the moment a post holder takes up duties at Eurojust until (s)he departs.
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).]	The PIFs are further dispatched to the relevant National Security Authorities who carry out the security screening.

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 Personal Information Forms received by the Clearance Office and the certificates/assurances for access to EU classified information are subject to secure handling and physically protected in a safe with restricted access. The safe has a key and a combination which is changed every 12 months or when there is a change in post holders knowing the combination. The Clearance Records are stored on DMS with restricted access and only the Head of Security and the Clearance and Registry Officer have access to them.
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 (file attached to this record)