




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 - <u>Active Directory (AD) Office Network</u>
To manage user accounts and their rights in context of IT systems.		
1.	Last update of this record	10/12/2019
2.	Reference number [For tracking, please contact the DP Office for obtaining a reference number.]	IMU-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 IM IMSecretariat@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

Nr.	Item	Description - <u>Active Directory (AD) Office Network</u>
6.	<p>Name and contact details of processor (where applicable)</p> <p>[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).]</p>	<p><u>usersupport@eurojust.europa.eu</u> - creates the initial AD account.</p> <p><u>am@eurojust.europa.eu</u> – Application Managers add additional group memberships</p> <p><u>backoffice@eurojust.europa.eu</u> – Assists with one off (unusual) requests</p>
7.	<p>Purpose of the processing</p> <p>[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).]</p>	<p>To manage user accounts and their rights in context of IT systems. The underlying purpose is to ensure the appropriate level of security is applied in a consistent fashion across Eurojust's IT services with the ability to identify the users of the service and/or determine their authorizations and roles within the context of their service.</p>
8.	<p>Description of categories of persons whose data are processed and list of data categories</p> <p>[In case data categories differ between different categories of persons, please explain as well.]</p>	<p>All Eurojust post holders: including JITs members, State Connection Members, Consultants, interns and trainees.</p> <ol style="list-style-type: none"> 1) Name, Title, email address, Password, Job title, ND, Unit/Service, Office phone number, Mobile number, Location, SIP (Session Initiation Protocol) address, Picture, Organisation. 2) Name, Title, email address, Office, Picture, Office Phone Number, Location, Department, Function. <p>The extended information from the first category is accessible only to User Support, Back Office and Application Managers.</p> <p>The information from the second category is accessible to all Eurojust post holders with active Active Directory account.</p>
9.	<p>Time limit for keeping the data</p> <p>[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).]</p>	<p>Data created by the system in respect to an individual person is maintained as long as the person is active. Once no longer active, data is retained for 7 years.</p>

Nr.	Item	Description - <u>Active Directory (AD) Office Network</u>
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).]	1) User Support, Back Office, Application Managers 2) All Eurojust users with active account may access personal data stored in the Active Directory The first category of recipients can access additional information referred to in section 8 point 1. The second category of recipients can access the information specified in section 8 point 2.
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.]	Active Directory is protected through measures defined in Eurojust ICT Policies and Procedures and industry best practices. <u>Security controls</u>
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  Data_Protection_Notice_AD_2019.docx