




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 – Eurojust Mobile Phones
<p>Enable authorized Eurojust post-holder to use their mobile phones, monitor the functioning of the phones for user and policy compliance, troubleshooting and, if needed, to enable ICT Security investigations on the infrastructure used to manage the mobile phones.</p>		
1.	Last update of this record	19/07/2022
2.	<p>Reference number</p> <p>[For tracking, please contact the DP Office for obtaining a reference number.]</p>	
3.	<p>Name and contact details of controller</p> <p>[Use functional mailboxes, not personal ones, as far as possible - this saves time when updating records and contributes to business continuity.]</p>	<p>Head of IM Unit</p> <p>mchanfreau@eurojust.europa.eu</p>
4.	Name and contact details of DPO	dpo@eurojust.europa.eu
5.	<p>Name and contact details of joint controller (where applicable)</p> <p>[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.]</p>	Not Applicable
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,</p>	<p>usersupport@eurojust.europa.eu – initial troubleshooting</p> <p>backoffice@eurojust.europa.eu – system performance monitoring, troubleshooting and reconstruction of</p>

Nr.	Item	Description – Eurojust Mobile Phones
	please indicate so (e.g. 360° evaluations, outsourced IT services or pre-employment medical checks).]	events
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>The purpose of processing personal data are:</p> <ul style="list-style-type: none"> • Enable the use of mobile phones for authorized Eurojust post-holders • Troubleshoot, analyse and resolve technical issues related to the working of the mobile phones and/or the underlying infrastructure • Detect performance issues on the mobile phones infrastructure • Detect and identify possible unauthorised access to the mobile phones or to the Eurojust systems accessible by the mobile phones, including monitoring and detecting potential external security threats to the Eurojust infrastructure accessible via the mobile phones • Ensure mobile phones compliance with Eurojust regulations and policies
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>Data subjects with an allocated Eurojust Mobile Phone:</p> <ul style="list-style-type: none"> • Active Directory User name, • Email address • Time and date of accessing Eurojust ICT devices and systems, external IP address of user devices, translated internal IP address. • Technical Events Logs
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><u>Blackberry Server</u> – retention period is 3 months</p> <p>The retention period for Audit log is defined by the POLICY- Audit log as approved by the AD 08/03/2018.</p>
10.	<p>Recipients of the data</p> <p>[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</p>	User Support, Back Office

Nr.	Item	Description – Eurojust Mobile Phones
	course of a particular investigation (e.g. OLAF, EO, EDPS).]	
11.	<p>Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?</p> <p>[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.]</p>	No
12.	<p>General description of security measures, where possible.</p> <p>[Include a general description of your security measures that you could also provide to the public.]</p>	<p>Log file data is protected through measures defined in Eurojust Policies and Procedures and industry best practices.</p> <p>Security controls</p>
13.	<p>For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the data protection notice:</p> <p>[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.]</p>	<p>Data subjects can exercise their rights to access, rectify, object, and data portability for the data collected by Eurojust (as listed under point 8) as described in the Data protection Notice.</p> <div style="text-align: center;">  <p>Data_Protection_Notice_Mobile Phones.pdf</p> </div>