



## 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
<b>Whistleblowing procedure at Eurojust</b>		
1.	Last update of this record	July 2020
2.	Reference number	AD-03 (July 2020)
3.	Name and contact details of controller	Administrative Director of Eurojust  Postal address: P.O. Box 16183 – 2500 BD The Hague The Netherlands Office address: Johan de Wittlaan, 9 2517 JR The Hague The Netherlands Email: <a href="mailto:adconfidential@eurojust.europa.eu">adconfidential@eurojust.europa.eu</a>
4.	Name and contact details of DPO	<a href="mailto:dpo@eurojust.europa.eu">dpo@eurojust.europa.eu</a>
5.	Name and contact details of joint controller	N/A
6.	Name and contact details of processor	N/A
7.	Purpose of the processing	The purpose of the processing is to carry out the procedure defined by the College Decision 2019-02 on Eurojust guidelines on whistleblowing by members of its staff.
8.	Description of categories of persons whose data are processed and list of data categories	The rules apply to every staff member working at Eurojust, irrespective of their administrative position or status, involved in a whistleblowing episode acting in good faith, who reports facts discovered in the course of or in connection with his or her duties which point to the existence of serious irregularities. While the whistleblowing rules do not strictly speaking apply to seconded national experts, trainees, interim staff and local agents, these categories of staff are also encouraged to make use of the arrangements set out in the and the whistleblowing guidelines and Eurojust undertakes to protect these categories of staff against retaliation if they do so in good faith.

Nr.	Item	Description
		<p>The data which will be used only for that processing are the relevant documents necessary to manage the whistleblowing procedure:</p> <ul style="list-style-type: none"> <li>• surname and first name (should the whistle-blower chooses to disclose it)</li> <li>• e-mail address (should the whistle-blower chooses to disclose it)</li> <li>• date and signature (should the whistle-blower chooses to sign the report)</li> <li>• The whistleblowing report where all unnecessary data will be erased</li> </ul>
9.	<b>Time limit for keeping the data</b>	<p>The time for which the complaint files may be kept is the following: Upon the closing of an initial investigation led by Eurojust, the data gathered to build the investigation will either be sent to OLAF if it concerns fraud or if not relating to fraud, dealt with through the appropriate channels within Eurojust.</p> <p>If a case is sent to OLAF and an investigation is opened, there is no need for Eurojust to keep the information for a longer period and Eurojust will delete the information without delay. For files on the basis of which an administrative inquiry or disciplinary procedure is opened by Eurojust, the information should be kept in line with the retention periods foreseen for those files (maximum of 10 years after the closure of the case in order to allow a harmonised application of the Staff Regulations as outlined in the <a href="#">record of processing activities in the context of administrative inquiries and disciplinary proceedings</a>). When the investigation has dismissed a report of whistleblowing, the data gathered to build the investigation will be retained for a period of 2 months after the final decision has been issued to all the parties involved.</p>
10.	<b>Recipients of the data</b>	<p>The recipients of the data depend on the option that a staff member chooses to report a serious irregularity and it could be:</p> <p><i>Internal whistleblowing</i></p> <ul style="list-style-type: none"> <li>- the staff member's immediate superior</li> <li>-the Administrative Director</li> <li>-the President of the College</li> <li>-OLAF</li> </ul> <p>In any case, the recipient of the information is in turn obliged to transmit the information thus received without delay to OLAF.</p> <p><i>External whistleblowing</i></p> <p>Upon receipt of the information reported internally, OLAF or Eurojust must give the whistleblower within 60 days of receipt of the information an indication of the period of time that it considers reasonable and necessary to take appropriate action. If no action is taken within that period of time, or if the whistleblower can demonstrate that the period of time set is unreasonable in light of all the circumstances of the case, he or she may make use of the possibility of external whistleblowing by bringing his concerns to the attention of the President of either the Commission, the Council, the Parliament or the Court of Auditors, or to the Ombudsman.</p>

Nr.	Item	Description
		<p>In addition, data recipients can also be the HR unit contact point to provide confidential and impartial guidance on, for example, whether the information in question is covered by the whistleblowing rules, which reporting channel may best be used for the information concerned, and which alternative procedures are available if the information concerned does not qualify for whistleblowing ('signposting'). They will also be able to tender advice and guidance to staff members on protective measures that the staff member may wish to seek following the reporting and support potential whistleblowers.</p> <p>In case the Administrative Director decides to launch an administrative inquiry, data may be disclosed to the Disciplinary Board, the investigator, the staff member responsible for the inquiry and other persons involved in the inquiry.</p> <p>If the staff member concerned contests the disciplinary decision, the disciplinary file may be referred to the Court of Justice of the European Union. Data may be sent to the Ombudsman, if the staff member concerned addresses a complaint.</p>
11.	<p><b>Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?</b></p>	No
12.	<p><b>General description of security measures, where possible.</b></p>	<p>Technical measures include storing the case files electronically in a restricted area of the Document Management System. All processing operations are carried out pursuant to existing policies describing access control to different Eurojust applications.</p> <p>Only persons with a legitimate 'need to know' for the purposes of this processing operation have access to the personal data.</p> <p>Organisational measures include the use of locked closets, confidential settings in the emails and printing with badging.</p>
13.	<p><b>For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the data protection notice:</b></p>	<p><a href="#">Data protection notice</a></p>