



## RECORD OF PERSONAL DATA PROCESSING

Art. 31 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 (henceforth the "Regulation")

Record n°

15-2022

*In accordance with Article 31 of Regulation 2018/1725, individuals whose personal data are processed by the Agency in any context whatsoever are to be protected with regard to the processing of personal data and the Agency has to keep records of their processing operations.*

*This record covers two aspects:*

- 1. Mandatory records under Art 31 of the Regulation (recommendation: make the header and part 1 publicly available)*
- 2. Compliance check and risk screening (initial; part 2 is internal only to the Agency, not published)*

*The ground for the record is (tick the relevant one):*

- Regularization of a data processing operation already carried out*
- Record of a new data processing operation prior to its implementation*
- Change of a data processing operation*
- Migration from notification to record.*

Internal Control Survey (ICS)	
1	<b>Last update of this record (where applicable)</b> N/A, as this is the first version of the record
2	<b>Short description of the processing</b> According to EACEA's internal control framework (Communication to the Commission from Commissioner Oettinger: Revision of the internal control framework C(2017) 2373 dated 19 April 2017) final related to Internal Control Principle 16, EACEA should assess the effectiveness of its internal control system at least once a year. As part of this assessment, a survey to staff and to managers is carried out on an annual basis regarding selected internal control issues. There are two sets of questions, one for staff and one for management. The survey is anonymous and no link will be made between the answers given and the identity of the participants. The staff participating to the survey is selected from a list provided by Unit R1, including all EACEA staff. The methodology and participation is prepared by EACEA's sector responsible for internal control issues and decided by the EACEA's RMIC. EACEA uses the survey results and

	comments made to analyse the effectiveness of its internal control system. As a follow-up of the control activity the survey's outcome will be used to publish a report and to set up an action plan with implementing measures, if deemed necessary.
<b>Part 1 - Article 31 Record</b>	
3	<b>Name of the Controller Unit(s) and/or function of person acting on behalf of the Controller</b>
	Controller: European Education, and Culture Executive Agency Unit: R2 Marco.CARNACCINI@ec.europa.eu.
4	<b>Contact details of the Data Protection Officer (DPO)</b>
	EACEA-data-protection@ec.europa.eu
5	<b>Name and contact details of joint controller (where applicable)</b>
	NA
6	<b>Name and contact details of processor (where applicable)</b>
	NA
7	<b>Purpose of the processing</b>
	EACEA should assess the effectiveness of its internal control system at least once a year. The survey allows for the assessment through the replies provided by EACEA staff and management.
8	<b>Description of the categories of data subjects</b>
	Whose personal data are being processed? In case data categories differ between different categories of persons, please explain as well (e.g. suspects vs. witnesses in administrative inquiries) <input checked="" type="checkbox"/> Agency staff (Contractual and temporary staff in active position) <input type="checkbox"/> Visitors to the Agency <input type="checkbox"/> Contractors providing goods or services <input type="checkbox"/> Applicants <input type="checkbox"/> Relatives of the data subject <input type="checkbox"/> Complainants, correspondents and enquirers <input type="checkbox"/> Witnesses <input type="checkbox"/> Beneficiaries <input type="checkbox"/> External experts <input type="checkbox"/> Contractors <input type="checkbox"/> Other, please specify:
9	<b>Description of personal data categories</b>

	<p><b>Indicate <u>all</u> the categories of personal data processed and specify which personal data are being processed for each category (between brackets under/next to each category):</b></p> <p><b>a) Categories of personal data:</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> in the form of personal identification numbers</li> <li><input type="checkbox"/> concerning the physical characteristics of persons as well as the image, voice or fingerprints</li> <li><input type="checkbox"/> concerning the data subject's private sphere</li> <li><input type="checkbox"/> concerning pay, allowances and bank accounts</li> <li><input type="checkbox"/> concerning recruitment and contracts</li> <li><input type="checkbox"/> concerning the data subject's family</li> <li><input type="checkbox"/> concerning the data subject's career</li> <li><input type="checkbox"/> concerning leave and absences</li> <li><input type="checkbox"/> concerning missions and journeys</li> <li><input type="checkbox"/> concerning social security and pensions</li> <li><input type="checkbox"/> concerning expenses and medical benefits</li> <li><input type="checkbox"/> concerning telephone numbers and communications</li> <li><input checked="" type="checkbox"/> concerning names and addresses (including email addresses)</li> <li><input checked="" type="checkbox"/> Other: please specify: <b>grade and unit</b></li> </ul> <p>Respondents are expected to reply to questions related internal control. Personal data may be voluntarily provided in the open questions by the respondents on their own initiative, but this is expected to be limited, it is not requested through the survey and would be purely incidental.</p> <p><b>b) Categories of personal data processing likely to present <u>specific risks</u>:</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> data relating to suspected offences, offences, criminal convictions or security measures</li> <li><input type="checkbox"/> data being used to evaluate personal aspects of the data subject (ability, efficiency, conduct)</li> </ul> <p><b>c) Categories of personal data whose processing is <u>prohibited</u>, with exceptions (art. 10):</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> revealing racial or ethnic origin</li> <li><input type="checkbox"/> revealing political opinions</li> <li><input type="checkbox"/> revealing religious or philosophical beliefs</li> <li><input type="checkbox"/> revealing trade-union membership</li> <li><input type="checkbox"/> concerning health</li> <li><input type="checkbox"/> genetic data, biometric data for the purpose of uniquely identifying a natural person</li> <li><input type="checkbox"/> concerning sex life or sexual orientation</li> </ul> <p><b>d) Specify any additional data or explanatory information on the data being processed, if any:</b> NA</p>
10	<b>Retention time (time limit for keeping the personal data)</b>

	<p>For the purpose of the current process, EACEA.R2.002 keeps the personal data in view of launching the survey, analyse its outcome, and establish the list of participants invited to take part in the surveys of the coming two years. The maximum retention time is 30 months from the launch of the survey.</p> <p><b>Indicate the period of storage:</b> 30 months from the launch of the survey</p> <p><b>Is any further processing for historical, statistical or scientific purposes envisaged?</b>  <input type="checkbox"/> yes <input checked="" type="checkbox"/> no</p> <p><b>If yes, indicate the further retention time:</b></p>
11	<p><b>Recipients of the data</b></p> <p>Access to personal data is given on a need-to know basis to the following recipients:</p> <ul style="list-style-type: none"> <li>• EACEA Director</li> <li>• Staff members from Sector R2.002 (Performance, Audit and Internal Control) as survey administrators.</li> <li>• Staff in the European Commission DG DIGIT as managing EU Survey IT tool.</li> </ul> <p>In addition, in case of control or dispute, personal data can be shared with and processed by the bodies charged with a monitoring or inspection task in application of Union law in compliance with the applicable data protection rules and within the scope of their tasks entrusted by the relevant legislation. This includes, in particular, the following recipients:</p> <ul style="list-style-type: none"> <li>- The European Court of Justice or a national judge as well as the lawyers and the agents of the parties in case of a legal procedure;</li> <li>- The European Anti-Fraud Office (OLAF);</li> <li>- The Internal Audit Service of the Commission</li> <li>- The Investigation and Disciplinary Office of the Commission (IDOC)</li> <li>- The European Court of Auditors</li> <li>- The European Ombudsman</li> <li>- The European Public Prosecutor's Office</li> <li>- EU courts and national authorities</li> </ul>
12	<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> <p><u>NO</u></p>
13	<p><b>General description of the technical and organisational security measures</b></p> <p>The system used for the survey is EU SURVEY, managed by the European Commission (DG DIGIT).</p> <p>The European Commission's IT systems used by the Agency abide by the Commission's security guidelines. The Agency must comply with Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission.</p> <p>1. Organisational measures:</p> <p>A Corporate Local Informatics Security Officer (C-LISO) is in place. Its role includes supervising the Agency compliance with the relevant regulations, and the application of security measures recommend by DIGIT.</p>

	<p>Organisational measures include appropriate access rights and access control. As a rule within the Agency, access to information systems, the file system or offices are subject to a series of authorisations where the person granting the access is different from the person requesting or authorising the access - except in limited cases of delegation. The responsible person in the unit in charge of this action (processing operation of the current record) collects and places the documents on the secured drives of the Commission and all Agency staff are bound by a confidentiality obligation. The 'need to know' principle applies in all cases.</p> <p>2. Technical measures:</p> <p>State of the art technical cybersecurity measures are implemented in the corporate systems, according to the security needs. Those measures are in constant evolution.</p>
14	<p><b>Information to data subjects / Data Protection Notice (DPN)</b></p> <p>The Data protection Notice is published in the EACEA internal control intranet page and linked to the survey itself.</p>