



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°

17-2022

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.*

EACEA Staff Committee Elections	
1	Last update of this record (where applicable) The relevant record was last updated in November 2022 (reference n 17-2022).
2	Short description of the processing This processing activity covers the processing of personal data in order to organise Staff Committee elections.

Part 1 - Article 31 Record

3	<p>Name of the Controller Unit(s) and/or function of person acting on behalf of the Controller</p> <p>The controller is the European Education and Culture Executive Agency (EACEA). For organisational reasons, the role of the data controller is exercised by the Head of Unit R1 ("People, Workplace and Communication") of the EACEA. The controller may be contacted via functional mailbox: EACEA-HR@ec.europa.eu</p>
4	<p>Contact details of the Data Protection Officer (DPO)</p> <p>EACEA-data-protection@ec.europa.eu</p>
5	<p>Name and contact details of joint controller (where applicable)</p> <p>NA</p>
6	<p>Name and contact details of processor (where applicable)</p> <p>HaDEA - European Health and Digital Executive Agency for the use of the e-election IT tool.</p>
7	<p>Purpose of the processing</p> <p>The purpose of the process is to organise the elections in order to set up the EACEA Staff Committee. The processing covers setting up of the electoral committee, extracting from Sysper and publishing the electoral roll, checking the eligibility of applications and publishing the list of candidates, organizing and supervising the voting process and setting-up of the staff committee members list.</p>
8	<p>Description of the categories of data subjects</p> <p>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)</p> <p><input checked="" type="checkbox"/> Agency staff (Contractual and temporary staff in active position)</p> <p><input type="checkbox"/> Visitors to the Agency</p> <p><input type="checkbox"/> Contractors providing goods or services</p> <p><input type="checkbox"/> Applicants</p> <p><input type="checkbox"/> Relatives of the data subject</p> <p><input type="checkbox"/> Complainants, correspondents and enquirers</p> <p><input type="checkbox"/> Witnesses</p> <p><input type="checkbox"/> Beneficiaries</p> <p><input type="checkbox"/> External experts</p> <p><input type="checkbox"/> Contractors</p>

	<input type="checkbox"/> Other, please specify:
9	Description of personal data categories
	<p>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):</p> <p><input checked="" type="checkbox"/> in the form of personal identification numbers: EU login</p> <p><input checked="" type="checkbox"/> concerning the physical characteristics of persons as well as the image, voice or fingerprints: photos of the candidates</p> <p><input type="checkbox"/> concerning the data subject's private sphere</p> <p><input type="checkbox"/> concerning pay, allowances and bank accounts</p> <p><input type="checkbox"/> concerning recruitment and contracts:</p> <p><input type="checkbox"/> concerning the data subject's family</p> <p><input checked="" type="checkbox"/> concerning the data subject's career: type of contract (Contract/Temporary staff), Unit and the start and duration of the contract</p> <p><input type="checkbox"/> concerning leave and absences</p> <p><input type="checkbox"/> concerning missions and journeys</p> <p><input type="checkbox"/> concerning social security and pensions</p> <p><input type="checkbox"/> concerning expenses and medical benefits</p> <p><input checked="" type="checkbox"/> concerning telephone numbers and communications</p> <p><input checked="" type="checkbox"/> concerning names and addresses (including email addresses): first name, last name and professional address</p> <p><input checked="" type="checkbox"/> Other: Office location (applicable only for paper voting).</p> <p>For the members of the Electoral Committee:</p> <ul style="list-style-type: none"> • Role in the respective committee (e.g. chairperson, member) <p>For the candidates:</p> <ul style="list-style-type: none"> • Motivation and priorities to address as a candidate <p>Access to the relevant modules of Sysper 2 to elaborate the list of electors and candidates is done on a need-to-know basis.</p> <p><i>b) Categories of personal data processing likely to present <u>specific risks</u>:</i></p> <p><input type="checkbox"/> data relating to suspected offences, offences, criminal convictions or security measures</p> <p><input type="checkbox"/> data being used to evaluate personal aspects of the data subject (ability, efficiency, conduct)</p> <p><i>c) Categories of personal data whose processing is <u>prohibited</u>, with exceptions (art. 10):</i></p> <p><input type="checkbox"/> revealing racial or ethnic origin</p> <p><input type="checkbox"/> revealing political opinions</p> <p><input type="checkbox"/> revealing religious or philosophical beliefs</p> <p><input type="checkbox"/> revealing trade-union membership</p> <p><input type="checkbox"/> concerning health</p>

	<input type="checkbox"/> genetic data, biometric data for the purpose of uniquely identifying a natural person <input type="checkbox"/> concerning sex life or sexual orientation <i>d) Specify any additional data or explanatory information on the data being processed, if any: _____</i>
10	<p>Retention time (time limit for keeping the personal data)</p> <p>EACEA applies by analogy the principles and the retention periods indicated in section 12.2.3, Annex 1 of the Common Commission-Level Retention List (SEC(2019)900)/3 which provides for a 10-year administrative retention period after the end of the election process.</p> <p>Exception is made with the electoral roll of those who meet the conditions to vote and to stand for elections available on the intranet, the ballots, and the application forms, which are kept until the end of the period established for challenging the elections.</p> <p>Data under the e-voting tool is kept by the data processor for 3 months after the elections of the EACEA staff committee. Upon expiry of this period, the processor shall, at the choice of the controller, return, without any undue delay in a commonly agreed format, all personal data processed on behalf of the controller and the copies thereof or shall effectively delete all personal data unless Union or national law requires a longer storage of personal data.</p> <p>Personal data will be kept beyond the time-limits indicated above where they may be required for consultation in the context of legal or administrative procedures (for example, requests by the Ombudsman, appeals to the Court of Justice etc.) which are still pending when the time-limit expires.</p> <p>The names of the elected Staff members remain in the dedicated page of Staff Committee as long as they remain elected and are removed as soon as the Staff members are no longer elected.</p> <p>Is any further processing for historical, statistical or scientific purposes envisaged? <input type="checkbox"/> yes <input checked="" type="checkbox"/> no</p>
11	<p>Recipients of the data</p> <p>All recipients are on a “need to know basis”.</p> <ul style="list-style-type: none"> • The electoral committee: to the electoral roll, candidates’ applications and list of candidates • EACEA staff members and to other European Institutions having access to the EACEA intranet: to the electoral roll, posters, announcements and data concerning the appointment of the Staff Committee. Also leaflets/brochures that could be placed (during the elections period) in public areas will be disclosed to staff having access to EACEA building. • Director of the Agency • HR Sector : i.e. technical support, etc. • HaDEA staff responsible for the technical management: in the case of electronic voting <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</p>

	<p>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"> • 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; • The European Anti-Fraud Office (OLAF); • The Internal Audit Service of the Commission • The Investigation and Disciplinary Office of the Commission (IDOC) • The European Court of Auditors • The European Ombudsman • The European Public Prosecutor's Office
12	<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>N/A</p>
13	<p>General description of the technical and organisational security measures</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>The use of electronic voting system is subject to EU login password. An Outlook functional mailbox is created and used solely for the elections organisation purposes. Just members of the electoral committee have access to this functional mailbox.</p> <p>Paper files are stored in locked cupboards that are only accessible to staff organizing the elections (electoral committee).</p> <p>The specific folder on the EACEA shared drive is accessible only to staff in charge of organising the elections.</p> <p>Decisions are stored in ARES with the relevant safeguards (access via ECAS password).</p> <p>The Intranet page is updated on a regular basis: once the elections are finished and the period established for challenging the elections over, the related information is deleted (e.g. electoral roll). The names of the elected Staff members remain in the dedicated page of Staff Committee as long as they remain elected and are removed as soon as the Staff members are</p>

	<p>no longer elected.</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>Information to data subjects / Privacy Statement</p> <p>The Agency will publish a privacy statement on the Staff Committee page on the Intranet.</p>