EUROPEAN COMMISSION
European Education, and Culture Executive Agency

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 nº	*2024-04*

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.*

Follow-up by the Agency of European Ombudsman inquiries	
1	**Last update of this record (where applicable)**
	N/A
2	**Short description of the processing**
	The Agency deals with inquiries and correspondence transmitted by the European Ombudsman in the framework of investigations by the latter into possible cases of maladministration. Inquiries from the European Ombudsman are sent to the Agency via "DECIDE", which is the IT tool managed by the European Commission's Secretariat-General and which is covered by a specific EC record, DPR-EC-00839.3. Access to " DECIDE " is given only to authorised staff. In accordance with EC rules on document management, all documents received and drawn up by the Agency, including correspondence, are registered in the ARES internal database (see specific EACEA record 2022-07 on document management for more

	information).
Part 1 - Article 31 Record	
3	Name of the Controller Unit(s) and/or function of person acting on behalf of the Controller
	Head of Unit B4 EACEA B4 - Operational Support and Business Processes North Light Building (SB34) Boulevard Simon Bolivar 34 BE – 1049 Brussels Email: EACEA-OMBUDSMAN@ec.europa.eu
4	**Contact details of the Data Protection Officer (DPO)**
	EACEA-DPO@ec.europa.eu
5	**Name and contact details of joint controller (where applicable)**
	Secretariat-General (SG) Unit C2: The European Commission (EC) and the Executive Agencies have signed a joint controllership agreement (Ref. Ares(2021)5396089-1/09/2021) setting out the allocation of respective responsibilities and practical arrangements.
6	**Name and contact details of processor (where applicable)**
	Not applicable
7	**Purpose of the processing**
	The purpose is to handle inquiries transmitted to the Agency by the European Ombudsman's office in the framework of investigations into possible cases of maladministration.
8	**Description of the categories of data subjects**
	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) ☒ Agency staff (Contractual and temporary staff in active position) ☒ Visitors to the Agency

	☒ Contractors providing goods or services ☒ Applicants ☐ Relatives of the data subject ☒ Complainants, correspondents and enquirers ☒ Witnesses ☒ Beneficiaries ☒ External experts ☒ Contractors ☒ Other, please specify: - Any citizens who have submitted inquiries to the European Ombudsman regarding alleged instances of maladministration, which the European Ombudsman has transferred to the Agency for an opinion, further information or possible follow-up; - Citizens whose name and/or other personal data are mentioned in the corresponding correspondence with the European Ombudsman, including possibly the personal data of individuals other than the complainant that the latter spontaneously provided in his/her inquiry; - European Ombudsman staff involved in handling the inquiry, staff of EC or other EU Agencies, if they are involved in the inquiry.
9	**Description of personal data categories**
	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): ***a) Categories of personal data:*** ☐ in the form of personal identification numbers ☐ concerning the physical characteristics of persons as well as the image, voice or fingerprints ☐ concerning the data subject's private sphere ☒ concerning pay, allowances and bank accounts ☒ concerning recruitment and contracts ☒ concerning the data subject's family ☒ concerning the data subject's career ☐ concerning leave and absences ☐ concerning missions and journeys ☒ concerning social security and pensions ☐ concerning expenses and medical benefits ☒ concerning telephone numbers and communications ☒ concerning names and addresses (including email addresses) ☒ Other: please specify: Any other personal data which is relevant and necessary for the inquiry processing.

	b) Categories of personal data processing likely to present <u>specific risks:</u> ☒ data relating to suspected offences, offences, criminal convictions or security measures ☒ data being used to evaluate personal aspects of the data subject (ability, efficiency, conduct) ***c) Categories of personal data whose processing is <u>prohibited</u>, with exceptions (art. 10):*** ☒ revealing racial or ethnic origin ☒ revealing political opinions ☒ revealing religious or philosophical beliefs ☒ revealing trade-union membership ☒ concerning health ☐ genetic data, biometric data for the purpose of uniquely identifying a natural person ☒ concerning sex life or sexual orientation ***d) Specify any additional data or explanatory information on the data being processed, if any:*** _N/A_____
10	**Retention time (time limit for keeping the personal data)** 5 years after closure of the file in accordance with the retention period established in the 2022 Common Retention List — under point 2.4.4. **Is any further processing for historical, statistical or scientific purposes envisaged?** ☒ yes no In accordance with the common Commission Retention List and after the 'administrative retention period' of 5 years, files concerning Ombudsman inquiries may be transferred to the Historical Archives of the European Commission for historical purposes.
11	**Recipients of the data** Access to the data will be given only on a need to know basis to : - Agency's authorised staff in charge of handling or involved in the inquiry in the Agency - Authorised staff in the European Commission's services and Executive Agencies, where applicable. In the framework of a particular inquiry, personal data can be shared with and processed by bodies that are not regarded as recipients but are 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: - 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 Public Prosecutor's Office - the European Data Protection Supervisor. - National authorities
12	**Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?**
	In case the Agency is requested to reply directly to the complainant, transfer of personal data to third countries may occur in case the EU citizen resides outside EU. The disclosure of personal data to an EU citizen residing outside the EU is done only if the conditions for an international transfer of Chapter V of the Regulation are met. Since the factual and legal circumstances, including the place of residence of the complainant, are different for each case, the application of the appropriate legal basis for the transfer (adequacy decision - Article 47 of the Regulation, application of appropriate safeguards- Article 48.2 and .3, or derogation for a specific situation – Article 50(1)(d) and (g) of the Regulation) has to be assessed on a case-by-case basis.
13	**General description of the technical and organisational security measures**
	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. 1) Organisational measures Inquiries from the European Ombudsman are sent to the Agency via "DECIDE", which is the IT tool managed by the European Commission's Secretariat-General. Access to "DECIDE" is given only to authorised staff. The EU staff abide by statutory, confidentiality requirements. All data in electronic format (e-mails, documents…) are stored on a secured drive with restricted access on a need to know basis. Electronic data resides including in "DECIDE" on the servers of the European Commission, which abide by strict security measures to protect the security and integrity of electronic assets (through User-ID and password, etc.). An Outlook functional mailbox is created and used solely for the purpose of handling Ombudsman inquires and access to this mailbox is restricted on a need -to -know basis to the staff members of the Legal Advice Team, the Ombudsman coordinator and other staff of the legal team designated to handle Ombudsman cases. Access to documents related to the Ombudsman complaint are stored in ARES with the relevant safeguards (access via ECAS password and authentication). Paper files related to European Ombudsman cases (which tend to become rare since the process is mainly digital) are kept in a locked cupboard accessible only to a limited number of authorised staff, on a strict need-to-know basis and subject to specific internal approval procedures.

	2. Technical measures: State of the art technical cybersecurity measures are implemented in the corporate systems, according to the security needs. Those measures are in constant evolution.
14	**Information to data subjects / Data Protection Notice (DPN)**
	A Data Protection Notice (DPN) relevant to this data processing activity is available on the EACEA Intranet page for legal support in the section on Ombudsman) and on the EACEA website. In addition, complainants seeking information about the processing of their personal data will receive the DPN.

ANNEX

When to perform a Data Protection Impact Assessment (DPIA)

- **Data Protection Impact Assessment (DPIA)**

  You will not have to do DPIAs for all processing operations. Only those that are likely to pose a 'high risk to the rights and freedom of data subjects' require a DPIA. As the person responsible on behalf of the controller, preparing the DPIA is your task, assisted and guided by the DPO.

  The EDPS shall establish and make public a list of "kinds of processing operations" subject to a DPIA. The EDPS may also establish a negative list of kinds of processing operations not subject to DPIAs.

  You have to carry out a DPIA when your process meets at least one of the criteria below:

  (1) it is on the list of kinds of risky processing operations to be issued by the EDPS;
  (2) it is likely to result in high risks according to your threshold assessment

- **Threshold assessment**

  For processing operations that do not figure on the list for mandatory DPIAs, but which you and/or DPO still suspect may be high risk, conduct a threshold assessment using the template included in this document. In general, if you tick two or more of the criteria, you should do a DPIA. However, the assessment cannot be reduced to a simple calculation of the number of criteria met. This is not an automated decision. Indeed, in some cases, a processing meeting only one of these criteria may require a DPIA. In other cases, a DPIA may not be necessary despite meeting two or more criteria. If you tick two or more criteria and do not consider that the processing would in fact cause high risks for the persons affected, explain why after consulting the DPO.

- **EDPS Positive/negative lists**

  Below you may find the positive and negative lists (indicative) issued by EDPS. These lists are non-exhaustive (and not yet official) and aim at providing some guidance in the interim period.

  A) Positive list of processing operations prima facie requiring a DPIA (the numbers in brackets refer to the criteria in the threshold assessment such processing operations will likely trigger):

- Exclusion databases (2, 4, 9);
- large-scale processing of special categories of personal data (such as disease surveillance, pharmacovigilance, central databases for law-enforcement cooperation) (1, 4, 5, 8);
- internet traffic analysis breaking encryption (1, 3, 8).

B) Indicative list of processing operations prima facie *not* requiring a DPIA:

- Management of personal files as such[1];
- Standard staff evaluation procedures (annual appraisal);
- 360° evaluations for helping staff members develop training plans;
- Standard staff selection procedures;
- Establishment of rights upon entry into service;
- Management of leave, flexitime and teleworking;
- Standard access control systems (non-biometric);

[1] Some procedures resulting in adding information to the personal file may require DPIAs, but not the repository of personal files as such.

- Standard CCTV on a limited scale (no facial recognition, coverage limited to entry/exit points, only on-premises, not in publicly accessible space).