



RECORD OF PERSONAL DATA PROCESSING

Art. 31 of the *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°

Process: Domain Specific Facts

64

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

This record covers the following processes:

- 1) Mandatory records under Art 31 of the Regulation
- 2) Compliance check and risk screening

The ground for the record is:

- Regularization of a data processing activity already carried out.
 - Record of a new data processing activity prior to its implementation.
 - Change of a data processing activity.
 - Adaption of Agency's own record.
-

PART 1 (This part is made public) Name of the processing operation		
1	Creation and last update of this record (if applicable)	NA
2	Title and one-sentence description of the processing	Domain Specific Facts (DSF) Registration, assessment and validation management of domain specific facts related to participants for the purpose of participation to EU grants, prizes, procurement and activities via the EU Funding & Tenders Portal (hereinafter 'Portal')
Art 1 - Article 31 Records of processing activities		
2a	Legal basis	The processing is necessary <ul style="list-style-type: none"> - for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body (Article 5(1)(a) of the Regulation) - for the management and functioning of the Union Institutions or bodies (Recital (22) of the Regulation) - for compliance with a legal obligation to which the controller is subject (Article 5(1)(b) of the Regulation) - for the performance of a contract to which the data subject is party (Article 5(1)(c) of the Regulation)¹.
3	Function and contact details of the controller	The controller is the European Research Executive Agency (REA), represented by its Director. For organisational reasons, the role of the data controller has been entrusted by the Director to the delegated controller and is exercised by REA Head of Department B - Green Europe. The data controller may be contacted via functional mailbox: REA-LEGAL@ec.europa.eu

¹ The legal basis under Article 5(1) of the Regulation:

- (i) Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council of 23 September 2024 on the financial rules applicable to the general budget of the Union (hereinafter "the Financial Regulation") (OJ L , 2024/2509, 26.09.2024, ELI: <http://data.europa.eu/eli/reg/2024/2509/oj>.) and in particular: Title V (Common Rules), Title VII (Procurement and Concessions), Title VIII (Grants), Title IX (Prizes), Title XII (Other Budget Implementation Instruments, including management of experts and participant registration and validation) and Annex I (Procurement)
- (ii) The financing decisions form part of the legal basis for a processing operation, where applicable, in line with Article 110 of the Financial Regulation
- (iii) European Union law setting up specific funding programmes and initiatives is providing further legal basis for personal data processing but making reference to the Financial Regulation for actual implementation mechanisms
- (iv) European Union law establishing the EUIBAs as Joint Controllers

Additional legal basis:

- (v) The Terms & Conditions of the Funding & Tenders Portal (available at <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/support/legalnotice>)
- (vi) Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF)
- (vii) Council Regulation (Euratom, EC) No 2185/96 of 11 November 1996 concerning on-the-spot checks and inspections carried out by the Commission in order to protect the European Communities' financial interests against fraud and other irregularities
- (viii) Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office

4	Contact details of the Data Protection Officer (DPO)	REA-DATA-PROTECTION-OFFICER@ec.europa.eu
5	Name and contact details of joint controller (where applicable)	<p>Joint controllership is involved Yes</p> <p>The joint processing operations consist of the following processing activities:</p> <ul style="list-style-type: none"> - Definition of purposes and design of the related means (business processes and IT systems) for processing operations related to the management of contracts via the SEDIA corporate initiative - Registration, (re)assessment and (re)validation of participants in grants, prizes, and public procurement procedures: <ul style="list-style-type: none"> ▪ validation of legal existence of participants, their legal status and contact data; ▪ validation of decision-making and delegation rights of participants' legal representatives; ▪ preparation of participants' financial capacity; ▪ preparation of participants' ownership and control assessments; ▪ encoding of bank account and legal entity files into the Commission's accounting system <p>The essence of the Joint Controllership Arrangement is available here</p> <p>The full list of Joint Controllers is available here</p>
6	Name and contact details of processor (where applicable)	<p>Processors are involved in the processing</p> <p>No</p>
7	Purpose of the processing	<p>This record covers the processing of personal data collected for the purpose of managing EU programmes, procurement and activities via the EU Funding & Tenders Portal (hereinafter "the Portal") and the related processing operations undertaken for the purpose of domain specific facts registration, assessment and validation management inherent to the execution of the programmes managed by REA. More specifically, REA departments collect and use personal data to execute the EU Funding & Tenders Portal (hereinafter 'the Portal') business processes for (potential) participants in the EU funding programmes and activities managed by the REA. This record covers the personal data that the REA departments process, via the Portal, for the purpose of the processing operations relating to the Domain Specific Facts (DSF) registration, assessment, and validation management. The DSF (accreditations; affiliations; exemptions; and special cost methods) registration, assessment and validation of some participants is needed as, besides the 'core facts' of legal entities (common to all grants and procurement actions), several programmes need to request entities for specific data inherent to the execution of their programmes. In other words, DSF are facts about an organisation that are relevant only in specific contexts, not for all programmes. A DSF is always linked to a Participant Identification Code (PIC). All DSF are managed and validated by the relevant programme responsible, following a request from the REA services for additional information addressed to the concerned entities. The Personnel Unit Cost Audit Certificate (under the special cost methods) contains</p>

		<p>personal data of auditors; independent officers; or authorised representatives of audit firms.</p> <p>The Domain Specific Facts (accreditations; affiliations; exemptions; and special cost methods - Additional organisation data - IT How To - Funding Tenders Opportunities) validation, of some participants is needed, because besides the ‘core facts’ of legal entities common to all grant programmes and procurement actions, several programmes may need to request entities for specific data logic in the execution of their programmes.</p>
8	<p>Description of the categories of data subjects</p>	<ul style="list-style-type: none"> • Staff of European Union Institutions Bodies and Agencies (including officials, officials on probation, temporary agents, contractual agents, trainees) having a need to know and working with the participant related data either for validation or assessment or staff working with IT-developments or staff needing to consult the Participant Register data for their tasks. • Natural persons whose personal data is needed or embedded in the documents on the basis of which the validation / assessment of domain specific facts takes place, notably auditors, independent officers, authorised representatives of audit firms, etc.
9	<p>Description of personal data categories</p> <p>Indicate all 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>The categories of personal data are mentioned in the Personnel Unit Cost Audit Certificate on Annual Personnel Costs and Work Units, supporting the Special cost methods Domain Specific Fact:</p> <p>Identification data: (1) first name, middle name & last name (2) title (3) signature</p> <p>Contact data: (1) e-mail (2) contact (phone) numbers – including all types, such as: personal, business, GSM, landline, fax, voice over IP) (3) personal address(es) submitted (such as origin, permanent, current, previous residences)</p> <p>Employment related data: Function/position/employment status</p> <p>Other incidental and unsolicited data</p> <p>The data categories listed above are exhaustive, but the listed data fields are non-exhaustive.</p>
10	<p>Retention time (time limit for keeping the personal data)</p>	<p>The Joint Controllers only keep personal data for the time necessary to fulfil the purpose of collection or processing, namely for the following periods:</p>

Data category	Retention period	Start date/moment	End date/moment
Domain Specific Facts	For personal data in Domain Specific Facts	End of the year (31/12/YYYY) following the closure of the grant action or agreement or last financial / accounting operation of the grant agreement of the Participant -whichever is later (N)	N+10 years
	For personal data in Domain Specific Facts of the entities not signing a grant	End of the year of the call deadline (N)	N+5 years
	Scientific staff data present in the Domain Specific Facts (if any): limited categories of personal data of scientific staff of applicants/beneficiaries (i.e.: identification (<i>title, name, surname or Researcher ID</i>) and contact details (<i>e-mail</i>)) for scientific research and/or statistical purposes.	End of the year (31/12/YYYY) following the closure of the grant action or agreement or last financial / accounting operation of the grant agreement of the Participant -whichever is later (N) OR End of the year of the call deadline (N)	N+25 years
	These limited categories of personal data are retained pursuant to Article 4(1)(e) of the EU DPR, and subject to the implementation of appropriate safeguards in accordance with Article 13, unless the concerned applicant/beneficiary exercises the right to object under Article 23 of the EU DPR.	- whichever is later	

The Retention Period is based on the Common Commission-level retention list for European Commission files.

Is any further processing for archiving purposes in the public interest historical, statistical or scientific purposes envisaged?

yes; archiving in the public interest is not incompatible with the initial purposes, as the processing for the purpose other than that for which the personal data have been collected is based on Union law, which constitutes a necessary and proportionate measure in a democratic society. The processing of personal data for archiving purposes in the public interest is subject to appropriate safeguards for the rights and freedoms of the data subject pursuant to the Regulation. Those safeguards ensure that technical and organisational measures are in place in order to ensure, in particular, the principle of data minimisation. The operational controller is systematically assessing whether the same purpose can be achieved through anonymised data. The following further processing operations working with personal data collected through the Portal are listed below, with their separate data processing records and privacy statements: European Commission's Identity Access Management Service (IAMS), including EU Login, enabling registration & access to the Portal to internal and external users (data subjects): <https://ec.europa.eu/dpo-register/detail/DPR-EC-03187>; Management and (short- and medium-) term preservation of documents: <https://ec.europa.eu/dpo-register/detail/DPR-EC-00536>; Long-term preservation of the archives: in the rare occurrence that a file is selected or sampled at the end of retention period, some data may be retained in the Commission's Historical Archives as required by the Archives Regulation (Council Regulation No. 354/83): <https://ec.europa.eu/dpo-register/detail/DPR-EC-00837>; Early Detection and Exclusion System (EDES): a database for protection of the EU financial interests by means of detection of risks and imposition of administrative sanctions: [DPR-REA-34](#)

<p>11</p>	<p>Recipients of the data</p>	<p>Within the European Union organisation (the Joint Controllers / the EUIBA), a recipient may be:</p> <p>(i) any legal person that is an EUIBA who works with the Portal processing operations covered by this privacy statement or is entitled by law and</p> <p>(ii) any legal or natural person who is in a contractual relationship with an EUIBA who works with the Portal processing operations covered by this privacy statement. Such as staff of European Union institutions and bodies, external experts and staff of contractors</p> <p>Outside the European Union organisation, a recipient may be:</p> <p>(i) any legal or natural person to whom EUIBA is under regulatory duty or who needs it in the public interest and the recipient needs it for legitimate performance of tasks within its competence. Such as authorised persons representing EU Member States / EEA countries (and for associated countries if relevant for the programme) in various programming / legislative bodies (like programme committees, advisory groups, national authorities / agencies / contact points, etc.) and authorised persons representing industry in case of EU joint undertakings' operations, etc.</p> <p>(ii) any legal or natural person who has a contractual relationship with an EUIBA and who is working on behalf of and under the responsibility of the Joint-Controllers for the purposes of performing the tasks of the relevant contract or has a need-to-know stemming from the contract. Such as staff of contractors acting as processors for a specific processing operation (auditor, event organiser) external auditors / contractors carrying out financial verifications, etc.</p> <p>Further specific disclosure</p> <p>(iii) Specifically for procurement and grant management: partner organisations chosen by participant and included in participant's grant or tender proposal.</p> <p>(iv) Finally, in accordance with the Financial Regulation (particularly Article 38 et al), certain information on recipients of EU funds is published annually on the Europa webpage (Financial Transparency System: https://ec.europa.eu/budget/fts/index_en.htm; the Official Journal of the European Union and/or on the applicable website of the EUIBA).</p> <p>(v) Pursuant to Article 3(13) of the Regulation (EU) 2018/1725, public authorities which may receive personal data in the framework of a particular inquiry in accordance with European Union or Member State law shall not be regarded as recipients. The further processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.</p> <p>Pursuant to Art 3(13) of the Regulation, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or MS law shall not be regarded as recipients; the processing of those data by</p>
------------------	--------------------------------------	---

		<p>those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.</p> <p>Disclosure to recipients is exercised in compliance with the principles of “necessity” and “data minimisation”. The natural persons further abide by statutory obligations and, when required, additional confidentiality agreements. Recipients are reminded of their obligation to process the personal data provided to them only for the purposes for which they were transmitted.</p>
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>Data is transferred to countries outside the EU or EEA</p> <p>No, transfers do not occur and not planned to occur.</p> <p>Data is transferred to international organisation(s)</p> <p>No, transfers do not occur and not planned to occur.</p>
	<p><u>General</u> description of the technical and organisational security measures</p>	<p>All personal data in electronic format (emails, documents, databases, uploaded batches of data etc.) are stored on the servers of the Commission (with automatic backup and recovery mechanisms, as defined in the disaster recovery plan). All Commission IT systems (i.e. all Communication and Information Systems owned, procured, managed or used/operated by or on behalf of the Commission) are compliant with the Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission. In addition, external contractors run IT systems on behalf of the Commission in line with the provisions of Regulation 2018/1725. They act only upon written instructions from the Controllers and undertake to adopt appropriate technical and organisational security measures having regard to the risks inherent to the processing and to the nature of the personal data concerned. Appropriate technical and organisational security measures are in place to address all data processing risks (preventing unauthorised access, reading, copying, alteration or deletion of personal data etc.):</p> <p>Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into consideration the risk presented by the processing and the nature of the personal data being processed;</p> <p>Organisational measures include restricting access to personal data solely to authorised persons with a legitimate need-to-know for the purposes of this processing operation. Access to data is only available to registered users as approved by their hierarchy through a separate access control module managed by the Commission (EU Login and SECUNDA++), and according to the need-to-know principle. The security module logs which user has requested access to the system, together with the date and timestamp. Authentication is based on the EU Login mechanism.</p>

14	<u>Data subject rights/restrictions</u>	<p>A data subject can exercise his/her rights (Art 14-24 of the Regulation) by submitting a request concerning access, rectification, erasure, restriction or objection to processing of their personal data to the Controller (Article 14(3) of the Regulation) by sending their request to the functional email REA-LEGAL@ec.europa.eu.</p> <p>They may be restricted only under certain specific conditions as set out in the applicable <u>Restriction Decision</u> in accordance with Article 25 of the Regulation . Restrictions may also apply due to communication of a personal data breach or due to the confidentiality of electronic communications.</p> <p>Further to the above, data subjects may contact the REA Data Protection Officer (DPO): REA-DATA-PROTECTION-OFFICER@ec.europa.eu.</p> <p>In case of conflict, complaints can be addressed to the European Data Protection Supervisor: EDPS@edps.europa.eu.</p>
15	Information to data subjects/Data protection notice (DPN)	<p>A Data Protection Notice (DPN) relevant to this data processing is published on the REA public central register of records and also on the Portal here.</p>