Ref. Ares(2025)10646496 - 03/12/2025

European Research Council
Executive Agency

Established by the European Commission

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 "Data protection regulation"*)*

Record n°	DP 66/2025

In accordance with Article 31 of the data protection 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 two aspects:
1. Mandatory records under Art 31 of the data protection 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.*

(This part may be public) **Grant Management Procedure**		
1	**Last update of this record if applicable**	DPO 05-2011
2	**Short description of the processing**	This record covers the processing of personal data that the ERCEA obtained via the EU Funding & Tenders Portal (the 'Portal'), for the purpose of the processing operations relating to the award, management and follow-up of grants by the ERCEA in the context of implementing the EU funding programmes.
(This part may be public) **Part 1 - Article 31 Record**		
3	**Function and contact details of the controller**	Function: Director

		ERC-STG-GRANTING@ec.europa.eu ERC-COG-GRANTING@ec.europa.eu ERC-ADG-GRANTING@ec.europa.eu ERC-SYG-GRANTING@ec.europa.eu ERC-POC-GRANTING@ec.europa.eu
4	**Contact details of the Data Protection Officer (DPO)**	ERC-DATA-PROTECTION@ec.europa.eu
5	**Name and contact details of joint controller (where applicable)**	For the managing of the IT tool: DG DIGIT; DG RTD. REA for the validation of the legal entity. The contact details and the list of the other joint controllers, where applicable, can be found here.
6	**Name and contact details of processor (where applicable)**	External organisation(s)/entity(ies): The processors are the independent expert evaluators, monitors and other contractors who are working on behalf of and under the responsibility of the ERCEA for the purposes of proposal evaluation; grant management (including checks and reviews); external audits; action reporting; and Research networking.
7	**Purpose of the processing**	This record covers the personal data, collected through the Portal for the purpose of the processing operations related to the award, management and follow-up of grants by the ERCEA in the context of implementing the EU funding programmes. The purpose of the processing operations relating to the award, management and follow-up of grants is to ensure that: 1. the ensuing grant agreements are concluded and implemented according to the contractual provisions and in conformity with the sound financial management of the EU budget; 2. the follow-up of projects aims at maximising the dissemination and exploitation of the research results; 3. the processing of information (meta-data; personal data; public/confidential information contained in proposals/results/reports/publications/deliverables of projects; and any further information) collected within the course of operations for the monitoring and evaluation of the EU funding programmes and initiatives is adequate and serves to the improvement of the future EU funding programmes and Initiatives; and 4. the actions and the provisions of the grant agreements are being properly implemented. This record covers the entire life cycle of linked personal data processing operations including (but not limited to), validation, entry into and monitoring of relevant type of legal commitment and all linked financial transactions. The record also covers all internal and external checks, audits, investigations and other proceedings that users of EU public funds are subject to assess the legality and regularity of the transactions underlying the implementation of the EU budget. The audit and control activities can be conducted at any time during the performance of the programme/project, as well as thereafter, and can concern any aspect (including beneficiaries; projects; systems; transactions etc.), depending on the needs of the ERCEA. The audit and

		control activities may be carried out on documents; and/or on the spot in any place where the funds in question are managed or used; the geographical scope is therefore worldwide. The record covers both external and internal data subjects (i.e. ERCEA staff). The ERCEA may use limited personal data obtained through the Portal for the purposes of: 1. monitoring, evaluating, and improving the programmes and initiatives; 2. to account for these in front of the legislative authorities (the European Parliament and the Council of the European Union); 3. to comply with their public reporting obligations; and as a source of information for policy-making. A limited subset of the personal data may be processed for communication purposes, as per the rules of each call for proposals. The ERCEA will additionally process certain personal data of PIs to verify if the PIs are currently involved in an ongoing ERC project. The processing of the personal data of ERCEA staff is necessary for the access to the tools used for the grant management (e.g. COMPASS), for carrying out the assigned tasks to assess the legality and regularity of the transactions underlying the implementation of the EU budget and to keep record of the performed actions for audit purposes. Personal data may be used for training and testing AI-driven models for enhancing and refining the expert data base (e.g. to suggest matching expertise), to this end, see the following. ERCEA will further process the personal data, other than for which the personal data were initially collected, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.
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) x☒ EA staff (Contractual and temporary staff in active position ☐ Visitors to the EA x☐ Contractors providing goods or services x☒ Applicants x☐ Relatives of the data subject ☐ Complainants, correspondents and enquirers ☐ Witnesses x☒ Beneficiaries

		x☐ External experts ☐ Contractors ☐ Other, please specify _____
9	**Description of personal data categories** 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):	*Categories of personal data:* ☒x in the form of personal identification numbers [Participant Identification Code (PIC); ID document number (passport or other); for ERCEA staff: user name] X concerning the physical characteristics of persons as well as the image, voice or fingerprints [Photos made available in CVs and identification documents] ☒ concerning the data subject's private sphere [Gender; title; nationality] ☒ concerning pay, allowances and bank accounts ☐ concerning recruitment and contracts ☒ concerning the data subject's family ☒ X concerning the data subject's career [Employment related data: current employment status (employer's name and address, department, function/position, staff category); employment contracts; salaries; timesheets; career stage] ☒ X concerning leave and absences [Parental leave, illness leave, sabbatical] X concerning missions and journeys [Mission related data: missions/meetings/minutes/reports from current employer; supporting documents related to travel costs] ☐ concerning social security and pensions ☐ concerning expenses and medical benefits X concerning telephone numbers and communications [Phone number (personal, business, mobile, landline, fax, voice over IP)] concerning names and addresses (including email addresses) [First, middle and last name (including maiden name); email; residential address (origin, permanent,

		current/previous); for ERCEA staff: first, middle and last name]. ☒ Other :please specify :_____ [Other personal identifiers linked to other sources, such as ORCID/Researcher ID] [Data necessary for management of procedural/evaluation/performance related aspects: eligibility criteria related personal data and programme related accreditation data; exclusion criteria related personal data (including declaration on honour); selection criteria related personal data; award criteria related personal data; performance related personal data linked to legal commitment with the ERCEA (such as quality of performance of participant (if a natural person) or participant's staff during the execution of relevant legal commitment with the ERCEA, information linked to participation in meetings); any other procedural (application, evaluation process related, project reporting and monitoring and etc.) data that is of personal nature and linked to points listed above (including role in the project)] [Authentication and access data: EU Login credentials; IP address; security data/log in files] [Search related data of logged in users: search history and recommendations preferences] *Categories of personal data processing likely to present <u>specific risks:</u>* ☒ data relating to suspected offences, offences, criminal convictions or security measures [In exceptional cases, only if personal data related to criminal convictions and offences is included in the evidence that may be requested by the Authorizing Officer Responsible to prove the absence of exclusion of the entity or related persons.] ☐ data being used to evaluate personal aspects of the data subject (ability, efficiency, conduct) *Categories of personal data whose processing is <u>prohibited</u>, with exceptions (art. 10 Regulation):* revealing racial or ethnic origin ☐ revealing political opinions ☐ revealing religious or philosophical beliefs ☐ revealing trade-union membership ☐ concerning health ☒ [information related to health conditions in relation to claims (e.g. for special costs or triggering a change for a contractual condition (suspension, amendment, illness leave, parental leave, etc.))] genetic data, biometric data for the purpose of uniquely identifying a natural person ☐ concerning sex life or sexual orientation ☐

		Data subjects are free to provide voluntary health-related data for obtaining additional reimbursement due to special needs and possible additional costs. In addition, in the course of its audit/control activities, the ERCEA and its processors might process special categories of personal data (related to maternity/illness/special leaves). Further incidental and/or unsolicited personal data may be referenced by the data subjects without the request of the ERCEA, such as: third-parties personal data (the supporting documents submitted by the data subjects may contain personal data of third-parties (such as other experts mentioned in proposals; board members, etc.) not necessary for purposes of processing in business areas of the Portal); data revealing racial/ethnic origin; political opinions; religious/philosophical beliefs; trade union membership; sexual orientation - if these data appear in the documents (CVs; ID documents; other documents) and references to personal data freely available on social networks and the Internet.
10	**Retention time (time limit for keeping the personal data)**	Personal data of unsuccessful applicants (including outdated versions or withdrawn proposals) are retained for a period of 5 (five) years after the end of the year of the call submission deadline. Personal data of beneficiaries who were rewarded with a grant are retained for a period of 10 (ten) years after the end of the year in which either the grant action/agreement was closed or the last financial/accounting operation of the grant agreement took place, whichever is later. Personal data of ERCEA staff will be retained for a period of 10 (ten) years after the end of the year in which the grant was closed; log files will be retained for 1 (one) year after the creation of the log. Is any further processing for archiving purposes in the public interest, historical, statistical or scientific purposes envisaged? ☒ yes ☐ Personal data (title; first and last name; researcher ID; email) of the scientific staff of the applicants and beneficiaries will be retained for a period of 25 (twenty-five) years after the end of the year in which either the grant action/agreement was closed or the last financial/accounting operation of the grant agreement took place, whichever is later (for the beneficiaries) for scientific or research purposes or statistical purposes. Explicitly for the purpose of detection of altered personal data in future applications and/or detection of plagiarism in future submitted proposals by same or other principal investigators, personal data will be retained for a period of 15 (fifteen) years after the closure of the call. The type of personal data that will be retained for the purpose above is: 1. Scientific Project data: technical annex to grants, continuous reporting data, including list of publications, etc, workforce data, periodic and final scientific reports to grants; 2. Financial Project data: financial structured data and financial reports; 3. Audit Information: audit reports, and checks and reviews.

		Explicitly for statistical purposes, personal data of the scientific staff and the beneficiaries will be retained for a period of 25 (twenty-five) years after the end of the year in which the call was closed. The type of personal data that will be retained for the purpose above is: 1. Scientific Project data: continuous reporting data, including list of publications, etc, workforce data; 2. Financial Project data: financial structured data; 3. Audit Information: checks and reviews; 4. Ex post Evaluation: evaluation scoring and results, expert reviews and identities. Explicitly for scientific research purposes, personal data of the scientific staff and the beneficiaries will be retained for a period of 25 (twenty-five) years after the end of the year in which the call was closed. The type of personal data that will be retained for the purpose above is audit information: checks and reviews. Explicitly for historical archive purposes, personal data of the scientific staff and the beneficiaries will be retained for an indefinite period of time. The type of personal data that will be retained for the purpose above is: 1. Scientific Project data: technical annex to grants, continuous reporting data, including list of publications, etc, workforce data, periodic and final scientific reports to grants; 2. Financial Project data: financial structured data; 3. Ex post Evaluation data: evaluation scoring and results, expert reviews and identities.
11	**Recipients of the data**	The persons with access to personal data are: 1. ERCEA employees, and all EC officers having access to COMPASS 2. Any natural or legal person with whom the ERCEA is under regulatory duty or who need personal data in the public interest or for legitimate performance of tasks within their competence (e.g. OLAF, EU Courts, Internal Audit Services of the Commission, Court of Auditors, European Ombudsman, EDPS); 3. The Scientific Council of the ERCEA which requires the data in the public interest for legitimate performance of tasks within its competence; 4. Any natural or legal person who needs the data in the public interest, if the recipient needs the data for legitimate performance of tasks within its competence in various programming/legislative bodies (e.g. EC staff having access to the corporate IT tools); 5. Any natural or legal person who has a contractual relationship with the ERCEA and who is working on behalf of and under the responsibility of the ERCEA for the purposes of performing the tasks of the relevant contract, or has a need-to-know stemming from the contract (external experts; authorised staff of contractors acting as processors for a specific processing operation (external auditors)). With explicit consent from the data subject, certain elements of personal data, such as the title and the acronym of the project, project website, the name of the researchers and the host institutions, will be made available for

		communication activities by ERCEA, for example, to inform of the results of the project.
12	**Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?**	Transfer outside of EU/EEA may occur in the context of: • evaluation/monitoring of grants by experts from non-EU/EEA countries; • sharing of grant information with National Contact Points and Programme Committee Members from non-EU/EEA associated countries. The transfer of personal data to countries outside the EU/EEA is justified on the basis of: 1. Art. 47 of the Regulation - the European Commission's adequacy decision; 2. Art. 48(2) of the Regulation – implementation of appropriate safeguards, such as standard data protection clauses. In case of the absence of an adequacy decision, or of appropriate safeguard, transfer of personal data to a third country or an international organisation is based on Art. 50(1), in particular clauses a, b, c and d: a: the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards; b: the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; c: the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; d: the transfer is necessary for important reasons of public interest.
13	**<u>General</u> description of the technical and organisational security measures**	All personal data on paper, if relevant, is stored in the premises of the Commission, access to which is controlled by access policies based on the Commission Decision (EU, Euratom) 2015/443 on security in the Commission. The paper files are stored in locked/secure cupboards and/or storage offices. Access is limited and is on a need-to-know basis. 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 Commission 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.): a. 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; b. 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 as Joint-Controller (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. The access rights for the accounting system are defined via the accounting system security modules. The authentication to the accounting system, the document management system etc. is accomplished via the EU Login mechanism, which is designed to increase the security of Commission's IT systems. The following measures are implemented to ensure the security and privacy of personal data when training the internal machine learning models to support the decision-making processes within the EU institutions: • Data Conversion: the personal data is converted to a numerical form prior to its use in machine learning model training; • Data Alteration: following the conversion process, the data undergo additional alterations to render the restoration of the original information impossible without incurring significant loss of information; • Pseudonymisation: the data alteration process employs pseudonymisation techniques (such as encryption, shuffling, and hashing) to protect the personal data.
14	**Information to data subjects/Specific Privacy Statement (SPS)**	The data protection notice for the use of the Portal is available here. The data protection notice on grant management is available here. The data protection notice regarding the joint controllers is available here.