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 nº 53-2021

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.*
☒ *Migration from notification to record.*

Identity Management Services

1	**Last update of this record if applicable**	Last notification of processing operation 04/10/2012 Ares(2012)1167168
2	**Short description of the processing**	User authentication, access control and authorisation for ERCEA and Commission information systems. This includes: • The European Commission Authentication Service (EU Login/ECAS); • The Commission Enterprise Directory (CED); • The Common User Directory (CUD) and Active Directory (AD). These systems, intrinsic to their function, use information such name, surname, email address and/or organisation.

Part 1 - Article 31 Record		
3	**Function and contact details of the controller**	ERCEA IRM ERC-IRM@ec.europa.eu COV2 25/P108 Tel. +32 229-67704
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)**	N/A
6	**Name and contact details of processor (where applicable)**	Directorate-General for Informatics (DG DIGIT) EC IAM SERVICE DESK
7	**Purpose of the processing**	Managing user populations and their rights in the context of IT systems. Ensuring the appropriate level of security is applied in a consistent fashion across ERCEA and Commission IT services with the ability to identify the user of the service and / or determine his or her authorisations and roles within the context of their service. A secondary purpose of the processing is to enable client applications to provide the following services: • "white pages" services, allowing users contact details to be found (e.g. e-mail address book or telephone directory) • selection of users from lists, usually based on some selection criteria • construction of lists of users, primarily e-mail distribution lists • customisation of user interfaces according to users' individual characteristics.
8	**Description of the categories of data subjects**	Users of ERCEA and Commission IT systems where it is necessary to know the identity of the user. Persons, not necessarily ERCEA or Commission personnel (example: Experts), whose contact details need to be available to users of ERCEA and Commission IT systems. See example below: ☒ EA staff (Contractual and temporary staff in active position including Seconded National Experts, interimaires, blue book trainees) ☐ Visitors to the EA

		☐ Contractors providing goods or services to the Agency ☒ Applicants ☐ Relatives of the data subject ☐ Complainants, correspondents and enquirers ☐ Witnesses ☒ Beneficiaries ☒ Independent experts ☒ Principal investigators (PI) ☒ Other Scientific staff ☐ Subcontractors ☒ Other, please specify: ERC stakeholders, such as supporting staff of the Scientific Council
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:* ☒ in the form of personal identification numbers ID 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) [Name, surname, professional email address]. ☐ Other :please specify : see examples below *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) *Categories of personal data whose processing is <u>prohibited</u>, with exceptions (art. 10 new Regulation):* ☐ 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 *Specify any additional data or explanatory information on the data being processed, if any:* Identifiers: three unique identifiers are stored. The username (or userid); the Commission personnel number (PER_ID) for internal users or, for automatically synchronised external users, a unique key; and the e-mail address (optional for external users). Other data: • Names; passwords; group membership; organisational assignment; telephone and office number; date password last changed; date of last authentication; account status (whether active, inactive or locked by an administrator); administrative status (activity and type of employment); job title; job functions; organisational role(s); occupation; place of work or residence; date of birth (used as matching criterion to prevent creation of duplicate entries for a single user). • Credentials. • Contact and location information. • Organisational status, assignment and functions. • Access rights (group membership and roles). • Authenticated account activity. • Error prevention information (to ensure correct matching of data between authoritative source and the identity repository). Account status.
10	**Retention time (time limit for keeping the personal data)**	Is any further processing for archiving purposes in the public interest, historical, statistical or scientific purposes envisaged? ☐ yes ☒ no Data created by the system in respect of an individual user is maintained as long as the user is active. Once no longer active, data is retained for a further year, to allow simpler reactivation of the user during that time. Thereafter, the data is rendered anonymous.

		Nevertheless, for personnel employed by or working for the Commission, the user's identifier (userid), PER_ID and, to prevent errors, dates of birth are not deleted in order to: (1) allow the reuse of the identifier, if appropriate, should the person require renewed access to Commission IT resources after a long absence. (2) determine the real world identity of a user. Systems relying on the authentication service may record the identifier used when performing an action - in cases of litigation, dispute or investigation, the personnel number linked to an identifier will be disclosed to an appropriate authority, subject to the prior authorisation of the Data Protection Officer. Since it is possible for users to change their identifiers, a history of changes must also remain accessible. The limited information is maintained for a period of three years.
11	**Recipients of the data**	• The Data is disclosed to the System Owner(s), System Supplier, Service Provider and the staff of the systems requiring Identity and Access Management. • Any ERCEA or Commission IT service registered within the Identity Management Service's database for the purposes described in Part 1, can access Data Subjects data. • Entities authorised by the Data Protection Officer to obtain historical data in justified cases where in the context of an investigation by the European Commission's DGs HR/DS, IDOC or by OLAF and/or an audit by IAS or CoA certain personal data can be requested by the investigators/auditors including data for which the ERCEA ICT is not the data controller. • Other systems forming part of the Identity Management Service. • Client applications within the ERCEA and Commission.
12	**Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?**	Not applicable.
13	**<u>General</u> description of the technical and organisational security measures**	**Physical security** (access to computer systems, quality of the file supports, public access or restricted access to locations, storage, transport of equipment, etc.) is enforced by access to backend infrastructure by badge and PIN only in DG DIGIT Data Centres. **Logical security** (coding control, undue removal or transmission of data, passwords, encrypted directories, backup, audit trails for data processing and communication, etc.) is enforced by audit trail on the databases remains if a change is made, MD5 encryption and access to only certain members of staff, protected by password.

14	**Information to data subjects/Data Protection Notice (DPN)**	The EU Login/ECAS statement is made available to end users on the following page: https://webgate.ec.europa.eu/cas/privacyStatement.html