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 DPO 39-2020

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*

Name of the processing operation
FILE MANAGEMENT AND BACK - UP MANAGEMENT OF THE ERCEA FILE SERVERS

1	**Last update of this record if applicable**	DPO 35-2012 [Ares(2012)937749]
2	**Short description of the processing**	**The ERCEA relies on an ICT infrastructure in order to ensure its mission. Shared network folders are used for safely storing and exchanging files internally among colleagues, who can be part of different teams/units/departments. Personal data are processed to enable end user collaboration services and to maintain the underlying infrastructure.** **Personal data are not used for an automated decision-making including profiling.** **The management of the Shared Drive is under the responsibility of DG DIGIT on behalf of ERCEA, which is responsible for ensuring that the IT aspects of business continuity are covered, from the daily back-up operations up to a full Disaster Recovery Planning.** **The present processing operation covers only the**

		aspects of the file server management and back-up of the IT infrastructure. For data which are not under the direct application of this record, separate records are finalised under the responsibility of the respective unit.
(This part may be public) **Part 1 - Article 31 Record**		
3	**Function and contact details of the controller**	Function: **Head of Unit** Unit : **ERCEA D1** e-mail address: **erc-irm@ec.europa.eu**
4	**Contact details of the Data Protection Officer (DPO)**	Functional e-mail address **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)**	**DIGIT C6** **DIGIT-C6@ec.europa.eu**
7	**Purpose of the processing**	Personal data are collected to enable Shared Network Folders in the context of the Digital Workplace programme for the agency staff. Shared network folders are used for safely storing and exchanging files internally. Personal data are processed to enable end user collaboration services and to maintain the underlying infrastructure as well as to manage access profiles for users and in order to guarantee so that files are accessible on a network drive on a need to know basis (only) and to prevent unauthorized access to the files. Personal data is not used for an automated decision-making including profiling.
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) ☒ 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 ☐ Applicants ☐ Relatives of the data subject

		☐ Complainants, correspondents and enquirers ☐ Witnesses ☐ Beneficiaries ☐ External experts ☒ On Site 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:* ☐ 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 :_____ *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:*
10	**Retention time (time limit for keeping the personal data)**	**The personal data is only kept for the time necessary to fulfil the purpose of collection or further processing. Name, username and unit as well as information about access rights are kept as long as a folder access permission is valid. No activity logs are kept. For what concerns the data on the users' home folders (personal folders (H:)), it is only retained as long as the data subject is a staff member of the ERCEA.** **The retention period for the files in the trash folder: files are automatically deleted every Sunday.** **For all data the retention period of the back-ups is 35 days.** **Concerning the personal data as described in the <u>files on the shared drive</u> (P:), the retention period of the data extends as long as it is needed, as indicated in the relevant record.** In case you intend to FURTHER process the personal data for a compatible purpose with the 'initial' one, please also indicate this retention period if different Is any further processing for archiving purposes in the public interest, historical, statistical or scientific purposes envisaged? ☐ yes ☒ no If yes, indicate the further retention time: … If the answer is yes, please go to Part 2 Compliance check, Storage and Security for technical safeguards.
11	**Recipients of the data**	**The recipients of the data are the ERCEA IRM team when verifying and approving the requests for access rights and DIGIT C6 when implementing the changes.** **Other than people mentioned in part 2 - point 2 "Detailed description of the Processing ", data may be disclosed to the ERCEA LISO (Local Information Security Officer) for security aspects and to Heads of Unit for the data related specifically to their unit or department's activities (example: information of HoU**

		B1 when 10.000 proposals and annexes had been stored on the file share). **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 (e.g. back-up of files).**
12	**Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?**	**NO**
13	**<u>General</u> description of the technical and organisational security measures**	**<u>Physical security</u>** **Back-ups are managed by DIGIT.C and are kept on systems running in their data centers. Access to these rooms is controlled and reserved to the members of the DIGIT LSA team who must use their badge in combination with a personal PIN code.** **DIGIT and the ERCEA ICT Unit implement the security rules in conformity with the policies and best practices used in the European Commission. In particular, it is bound by European Commission Decision C(2017)8841 of 13/12/2017 concerning the security of the information systems used by the European Commission and its implementing rules and guidelines.** **<u>Logical security</u>** **Access control is ensured through Active Directory managed by DIGIT LSAs. Please see part 2 - point 2 "Detailed description of the Processing ".**
14	**Information to data subjects/Data Protection Notice**	Please note that the information on the processing of personal data should always be sent or made available to the data subjects (existing SPS may need to be updated). **The data protection notice (DPN) is made available on on DIGIT Service Catalogue and a link is included in the ERCEA Intranet.**