

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°

DPO 51-2021

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

Name of the processing operation EMAIL service of the ERCEA		
1	Last update of this record if applicable	DPO 28-2012
2	Short description of the processing	It is necessary to process personal data in order to enable electronic communication and exchange of electronic messages and attachments amongst staff members and with external partners of the ERCEA. The processing operation is necessary in order to enable the staff of ERCEA to carry out their job. In addition, the ERCEA e-mail system offers to the user the e-mail access to addresses of all internal correspondents and of main external partners (other Institutions and bodies, Member states, etc.).
(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-DPO@ec.europa.eu
5	Name and contact details of joint controller (where applicable)	
6	Name and contact details of processor (where applicable)	DG DIGIT DIGIT-DPC@ec.europa.eu (Data Protection Coordinator)
7	Purpose of the processing	<p>Description of what you intend to achieve, meaning the reason and objective(s) for processing the personal data.</p> <p>The purpose of this processing operation is to provide the ERCEA staff with the proper communication tool to carry out the assigned job, which includes the management of the e-mail traffic from and to the mailboxes of ERCEA staff. Electronic mail, commonly known as email or e-mail, is a method of exchanging digital messages from an author to one or more recipients, which is necessary for performing the assigned tasks.</p> <p>The entire ERCEA email infrastructure is run as a service by DG DIGIT, European Commission, based on a Service Level Agreement signed with ERCEA.</p> <p>Modern email operates across the Internet or other computer networks. Today's email systems are based on a store-and-forward model. Email servers accept, forward, deliver and store messages. Neither the users nor their computers are required to be online simultaneously. The backend infrastructure relies on Microsoft Exchange and on the Global Address Book (GAL), a directory service within the Microsoft Exchange email system, for its functioning. The GAL contains contact information for all email users, distribution groups, and Exchange resources.</p> <p>Each e-mail system user has the responsibility for the messages and attachments he is processing and sending out.</p> <p>Components used by the user to access emails can be:</p> <ul style="list-style-type: none"> - Microsoft Outlook - Any standard HTTPS browser - Smartphones <p>Received e-mail messages in a Data Subject mailbox</p>

		<p>are under the user's full control, thus having all rights on these messages (like accessing, storing and deleting). Those rights do not apply to other copies of the same messages stored in somebody else's mailbox.</p> <p>Due to access rights reasons, Data Subjects cannot exert their rights concerning personal data directly in the E-mail System log-files.</p> <p>With regards to incorrectly encoded data in the Address Book, Data Subjects can take contact with the EC HELPDESK IT team who will redirect the users' requests to the competent team to correct faulty data.</p> <p>Data subjects have the possibility to send and receive encrypted and / or signed emails. Data subjects need to request their certificates to enable Secure Email.</p>
8	<p>Description of the categories of data subjects</p>	<p><input checked="" type="checkbox"/> EA staff (Contractual and temporary staff in active position)</p> <p><input type="checkbox"/> Visitors to the EA</p> <p><input type="checkbox"/> Contractors providing goods or services</p> <p><input type="checkbox"/> Applicants</p> <p><input type="checkbox"/> Relatives of the data subject</p> <p><input type="checkbox"/> Complainants, correspondents and enquirers</p> <p><input type="checkbox"/> Witnesses</p> <p><input type="checkbox"/> Beneficiaries</p> <p><input type="checkbox"/> External experts</p> <p><input checked="" type="checkbox"/> On Site Contractors</p> <p><input checked="" type="checkbox"/> Other, please specify SNE, Interims, blue book trainees_____</p>
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><i>Categories of personal data:</i></p> <p><input checked="" type="checkbox"/> in the form of personal identification numbers</p> <p>Staff number and usernames</p> <p><input checked="" type="checkbox"/> concerning the physical characteristics of persons as well as the image, voice or fingerprints</p> <p>Pictures</p> <p><input type="checkbox"/> concerning the data subject's private sphere</p> <p><input type="checkbox"/> concerning pay, allowances and bank accounts</p> <p><input type="checkbox"/> concerning recruitment and contracts</p> <p><input type="checkbox"/> concerning the data subject's family</p>

10	Retention time (time limit for keeping the personal data)	<p> <input type="checkbox"/> concerning the data subject's career <input type="checkbox"/> concerning leave and absences <input type="checkbox"/> concerning missions and journeys <input type="checkbox"/> concerning social security and pensions <input type="checkbox"/> concerning expenses and medical benefits <input checked="" type="checkbox"/> concerning telephone numbers and communications <input checked="" type="checkbox"/> concerning names and addresses (including email addresses) <input type="checkbox"/> Other :please specify :_____ </p> <p><i>Categories of personal data processing likely to present specific risks:</i></p> <p> <input type="checkbox"/> data relating to suspected offences, offences, criminal convictions or security measures <input type="checkbox"/> data being used to evaluate personal aspects of the data subject (ability, efficiency, conduct) </p> <p><i>Categories of personal data whose processing is prohibited, with exceptions (art. 10 new Regulation):</i></p> <table style="width: 100%; border: none;"> <tr> <td><input type="checkbox"/> revealing racial or ethnic origin</td> <td style="text-align: right;"><input type="checkbox"/></td> </tr> <tr> <td>revealing political opinions</td> <td style="text-align: right;"><input type="checkbox"/></td> </tr> <tr> <td>revealing religious or philosophical beliefs</td> <td style="text-align: right;"><input type="checkbox"/></td> </tr> <tr> <td>revealing trade-union membership</td> <td style="text-align: right;"><input type="checkbox"/></td> </tr> <tr> <td>concerning health</td> <td style="text-align: right;"><input type="checkbox"/></td> </tr> <tr> <td>genetic data, biometric data for the purpose of uniquely identifying a natural person</td> <td style="text-align: right;"><input type="checkbox"/></td> </tr> <tr> <td>concerning sex life or sexual orientation</td> <td style="text-align: right;"><input type="checkbox"/></td> </tr> </table> <p><i>Specify any additional data or explanatory information on the data being processed, if any:</i></p> <p>MAILBOXES - Kept for 4 months after the deletion of their owner's user account</p> <p>ADDRESS BOOK DATA: - as long as the Data Subject is an ERCEA staff member or ERCEA Contractor/Interiminaire, - as long as the Data Subject is present in the address book of the respective other Institutions, - After deletion from the on-line address book the retention period of Active Directory backups applies (cf ERCEA Record n° 41-2020 and DIGIT Record n° DPR-EC-3187).</p> <p>MESSAGES AND DOCUMENTS STORED IN MAILBOXES: - For Active Accounts, emails in the inbox are deleted after 6 months and in the other folders remain stored indefinitely until the Data Subjects deletes them manually, which is possible at any time. Emails are</p>	<input type="checkbox"/> revealing racial or ethnic origin	<input type="checkbox"/>	revealing political opinions	<input type="checkbox"/>	revealing religious or philosophical beliefs	<input type="checkbox"/>	revealing trade-union membership	<input type="checkbox"/>	concerning health	<input type="checkbox"/>	genetic data, biometric data for the purpose of uniquely identifying a natural person	<input type="checkbox"/>	concerning sex life or sexual orientation	<input type="checkbox"/>
<input type="checkbox"/> revealing racial or ethnic origin	<input type="checkbox"/>															
revealing political opinions	<input type="checkbox"/>															
revealing religious or philosophical beliefs	<input type="checkbox"/>															
revealing trade-union membership	<input type="checkbox"/>															
concerning health	<input type="checkbox"/>															
genetic data, biometric data for the purpose of uniquely identifying a natural person	<input type="checkbox"/>															
concerning sex life or sexual orientation	<input type="checkbox"/>															

		<p>backed up automatically for as long as they are in the user's mailbox.</p> <ul style="list-style-type: none"> - For Inactive Accounts, emails are kept for 4 months after the deletion of their owner's user account <p>MESSAGE OR DOCUMENT DELETED FROM A MAILBOX:</p> <ul style="list-style-type: none"> - These data are stored centrally for 30 additional days after deletion by the user <p>LOG FILES:</p> <ul style="list-style-type: none"> - Traffic log files are kept for 6 months. Anything that has to be kept longer (e.g. for statistical purposes) is anonymised. <p>Is any further processing for archiving purposes in the public interest, historical, statistical or scientific purposes envisaged?</p> <p><input type="checkbox"/> yes <input checked="" type="checkbox"/> no</p> <p>If yes, indicate the further retention time: ...</p> <hr/> <p>If the answer is yes, please go to Part 2 Compliance check, Storage and Security for technical safeguards.</p>
11	Recipients of the data	<p>Internal E-mail system users: European Commission and Executive Agencies' staff.</p> <p><u>Address book:</u></p> <ul style="list-style-type: none"> - Staff of the European Commission, - E-mail services of other European institutions. - Staff of other European institutions with whom bilateral agreements exist. <p><u>Log-files:</u></p> <ul style="list-style-type: none"> - Administrators of the E-mail System (daily operations), - HR.DS, IDOC, OLAF (on request in the context of investigations), - Data Subject concerned (on request). <p><u>E-mail messages:</u></p> <ul style="list-style-type: none"> - ERCEA and other European Institutions Users: EC staff and teams responsible for the email system and IT security - Outside the EU organisation: Mail recipients outside of the organisation (staff of other EU institutions, any other email recipient)

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>YES</p> <p>Proofpoint Inc. USA Personal data are mainly processed in Europe (the Netherlands and Germany). However, specific datasets (i.e. suspicious/unwanted emails, URLs and metadata related to these emails) may be processed in the US for analysis depending on the nature of their suspicious or threatening characteristics. The email solution used by ERCEA is operated and managed by DIGIT. Such solution does not allow ERCEA to choose or to exclude specific contractors.</p> <p>. Additionally, contractual safeguards are put in place. In the context of the continuous clean-up operations, the EC Email Service transfers selected email messages or individual attachments to external parties providing anti-malware services and tools (suppliers having a contractual relationship with the EC). Such transfers occur during the automatic traffic clean-up analysis, when users report inaccurate detections and exceptionally in the context of specific malware investigations. In the context of the troubleshooting of email systems incidents and problems, the EC Email Service transfers selected data to suppliers having a contractual relationship with the EC. The data actually transferred depends on the type of incident or problem.</p>
13	<p><u>General</u> description of the technical and organisational security measures</p>	<p><u>Physical security</u></p> <p>Email servers are managed by DIGIT.C and are kept in their data centres. 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.</p> <p>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 Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 concerning the security of the information systems used by the European Commission and its implementing rules and guidelines.</p> <p><u>Logical security</u></p> <p>The user needs to log onto the Windows Environment or onto the Outlook WebApp (available via https://myremote.ec.europa.eu and protected via a 2 way authentication methodology) to have access to his/her Email account.</p>
14	<p>Information to data subjects/Data Protection Notice</p>	<p>The details of the DPN are listed below in Point 7 of the following document. Processing operation: Email system of the European Commission Data Controller: DIGIT Record reference: DPR-EC-03610.1</p>