



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 ("Data Protection Regulation")

Record n°

DPO 40 - 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.

Business Continuity

Business Continuity		
1	Last update of this record if applicable	Business Continuity Plan (DPO 15-2012)
2	Short description of the processing	<p>Business continuity aims at ensuring the continuity of the operations and the service provided by the European Research Council Executive Agency (ERCEA) in case of events compromising the Agency's functioning. Such events may include the loss of premises, IT disruptions or the loss of staff (e.g. due to pandemics). In any such event, the corporate or ERCEA Business Continuity Plan (BCP) can be launched to respond to the respective circumstances in view of ensuring the continuity of critical and essential tasks. The collection of personal data puts the ERCEA in a position to face such crises and disruptive <i>force majeure</i> situations.</p> <p>The processing of personal data is therefore in the interest</p>

	<p>of both the organisation and its staff and complies with the principles of data minimisation and limited access. In very exceptional circumstances and on an ad hoc basis, sensitive data (such as health data and whereabouts outside the office) might be also processed.</p> <p>A further key aim in business continuity situations is to set benchmarks for operations and to monitor the Agency's activities in relation to those benchmarks. Specifically, business continuity management aims at verifying that all staff are safe, ensuring that they are able to work in stable conditions, minimising the risks related to the crisis event, structuring operations in a way to enable the running of the Agency's critical and essential functions and making possible the continuation of non-essential work.</p> <p>Personal data are collected through COMREF for the NOAH business continuity management (BCM) tool, to ensure swift communication, or directly from staff (e.g. with regard to their health data or safety). For the collection of specific data, BCM tools designed in-house may be used (e.g., for the recording of office presence or meeting participation).</p>
--	---

Part 1 - Article 31 Record

3	Function and contact details of the controller	ERCEA Director ERC-BCP@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)	n/a
6	Name and contact details of processor (where applicable)	Directorate-General for Informatics (DG DIGIT) DIGIT-SYSPER2@ec.europa.eu Directorate-General for Human Resources and Security (DG HR) HR-DATA-PROTECTION-COORDINATOR@ec.europa.eu Office for Infrastructure and Logistics (OIB) OIB-PROXIMITY-TEAM-MADO@ec.europa.eu OIB-55555@ec.europa.eu
7	Purpose of the processing	<p>Within the business continuity framework, the personal details of staff are used exclusively for the purpose of managing business continuity exercises or real events.</p> <p>The processing operation establishes an efficient two-way communication with staff and enables the follow-up of different requirements for setting up operations in such situations:</p> <ul style="list-style-type: none"> - Ensure a swift method of communication; - Ensure the safety and well-being of staff; - Organise the operations in a force majeure situation;

		<ul style="list-style-type: none"> - Identify and record whereabouts linked to business continuity (office, permanent residence at the place of employment, temporary residence, etc.) when necessary for the organisation of the operations; - Follow up on any guidelines or rules applicable to ERCEA staff by decision of the central Commission services, national authorities in Belgium or the ERCEA Director. <p>Moreover, the Data Controller may envisage anonymous statistical analyses with the purpose of improving the quality of the process.</p>
8	<p>Description of the categories of data subjects</p>	<p>Whose personal data are being processed?</p> <p><input checked="" type="checkbox"/> EA staff</p> <p>[Contract and Temporary Agents].</p> <p><input checked="" type="checkbox"/> Visitors to the EA</p> <p><input checked="" type="checkbox"/> Contractors providing goods or services</p> <p>[Intra-muros experts, interim staff].</p> <p><input type="checkbox"/> Applicants</p> <p><input checked="" type="checkbox"/> Relatives of the data subject</p> <p>[E.g. contact person indicated in SYSPER].</p> <p><input type="checkbox"/> Complainants, correspondents and enquirers</p> <p><input type="checkbox"/> Witnesses</p> <p><input type="checkbox"/> Beneficiaries</p> <p><input checked="" type="checkbox"/> External experts</p> <p>[Seconded National Experts].</p> <p><input checked="" type="checkbox"/> Other</p> <p>[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 type="checkbox"/> in the form of personal identification numbers</p> <p><input type="checkbox"/> concerning the physical characteristics of persons as well as the image, voice or fingerprints</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 checked="" type="checkbox"/> concerning recruitment and contracts</p> <p>[Start or end dates of active employment in the ERCEA].</p> <p><input checked="" type="checkbox"/> concerning the data subject's family</p> <p>[First and last name of contact person and their contact</p>

		<p>details].</p> <p><input type="checkbox"/> concerning the data subject's career</p> <p><input checked="" type="checkbox"/> concerning leave and absences</p> <p>[Telework / office presence days (regular or occasional), period of telework / office presence, comments related to the request].</p> <p>[Period and location of leave in case of pandemic situation].</p> <p><input checked="" type="checkbox"/> concerning missions and journeys</p> <p>[Mission status, period of mission, destination and purpose].</p> <p><input type="checkbox"/> concerning social security and pensions</p> <p><input type="checkbox"/> concerning expenses and medical benefits</p> <p><input checked="" type="checkbox"/> concerning telephone numbers and communications</p> <p>[Private home phone number, private mobile number].</p> <p><input checked="" type="checkbox"/> concerning names and addresses (including email addresses)</p> <p>[First and last name, private address, private e-mail address; office number(s); place of teleworking residence outside Belgium in case of pandemic situation].</p> <p><input checked="" type="checkbox"/> Other:</p> <p>[Only in case of special business continuity working modalities: date of in-office presence and work type (morning, afternoon, all day); date of encoding of presence and, if applicable, modification].</p> <p>[Participation in meetings; time, location and purpose of meetings].</p> <p><i>Categories of personal data processing likely to present <u>specific risks</u>:</i></p> <p><input type="checkbox"/> data relating to suspected offences, offences, criminal convictions or security measures</p> <p><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 <u>prohibited</u>, with exceptions (art. 10 new Regulation):</i></p> <p><input type="checkbox"/> revealing racial or ethnic origin</p> <p><input type="checkbox"/> revealing political opinions</p> <p><input type="checkbox"/> revealing religious or philosophical beliefs</p>
--	--	--

		<input type="checkbox"/> revealing trade-union membership <input checked="" type="checkbox"/> concerning health [Positive tests for contagious diseases of staff who were recently in a professional environment; the presence of symptoms compatible with infectious/contagious diseases as well as date of onset, if the symptoms appeared during or recently after a presence in the office; follow-up related to the aforementioned cases; in this context, the staff with whom symptomatic staff recently interacted in a professional environment]. <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 <i>Specify any additional data or explanatory information on the data being processed, if any:</i> Given the unforeseeable nature of crisis events, it is conceivable that further data categories, including sensitive data, may be processed. Moreover, staff members may reveal further data on a voluntary basis.
10	Retention time (time limit for keeping the personal data)	Personal data of staff is available in NOAH until the end of active service of staff in the ERCEA. Personal data related to health is stored the minimum necessary for no longer than two weeks after the end of the health situation. Is any further processing for archiving purposes in the public interest, historical, statistical or scientific purposes envisaged? <input checked="" type="checkbox"/> yes <input type="checkbox"/> no. The ERCEA may envisage anonymous statistical analyses with the purpose to improve the quality of the processes and the management of human resources.
11	Recipients of the data	The persons with access to your personal data, on a need-to-know basis , are: <ul style="list-style-type: none"> - The Agency's BC Correspondent, and the BC Desk Officer (and back-ups) can access the relevant staff data of all ERCEA staff; - BC Duty Officers (and back-ups) can access the relevant staff data of all ERCEA staff in case an event is initiated during their duty period; - Heads of service can access the personal data of any staff member of their entity in NOAH; - The members of the HR Unit and authorised personnel working to re-instate the functioning of operations, including in particular the Logistics and GECO teams; - Services of the European Commission: DG HR (e.g. health data), the Secretariat General (e.g., NOAH, record of meeting presence), DG DIGIT (as system administrator of NOAH), OIB (e.g. for disinfection arrangements of offices or common spaces), or IT teams responsible for creating tools;

		<ul style="list-style-type: none"> - The ERCEA's Director; - In highly exceptional situations, the national authorities of the host member state may receive specific information (e.g., in case of a missing staff member). <p>In addition, certain administrative details may be disclosed, in compliance with the relevant current legislation and established case law, and on a temporary basis to legislative or supervisory bodies of the ERCEA, as well as auditing bodies or courts.</p>
12	Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?	In exceptional cases, the personal data of staff may be transferred to the national authorities of third countries to establish the safety or security of ERCEA staff members (e.g. on mission) on the basis of the need to know principle and by complying with the specific conditions set up by the applicable data protection framework.
13	General description of the technical and organisational security measures	<p>The business continuity team is responsible for the management of any documents produced, circulated and/or received, ensuring the appropriate treatment of all documents.</p> <p>E-mails including personal data should be sent via encrypted e-mail (SECEM). Access to files is limited to authorised personnel, regardless of where they are saved: on the ERCEA Shared Drive; the Functional Mailbox (FMB) (ERC-BCP@ec.europa.eu); or of which a physical copy is kept.</p> <p>NOAH and any in-house monitoring tools guarantee a strict privacy protection of staff personal data through precise and stringent restrictions. Personal details are only displayed if the user has the right to access such data, as mentioned in point 1.11 above.</p>
14	Information to data subjects/Specific Privacy Statement (SPS)	<p>The Data Protection Notice is published on the ERCEA intranet "<i>Human Resources - Data Protection & Privacy</i>": http://intranet.ercea.cec.eu.int/services/human-resources/priv/Pages/default.aspx</p> <p>For information about business continuity in the ERCEA, visit the intranet: http://intranet.ercea.cec.eu.int/services/human-resources/working-environment/Pages/Business-Continuity-and-Emergencies.aspx</p> <p>For more information on Business Continuity Management within the Commission, you can visit the Business Continuity website.</p> <p>The privacy statement of the European Commission on business continuity may be found here: https://myintracomm.ec.europa.eu/sg/bcm/Documents/noah_privacy_statement.pdf</p>