EUROPEAN RESEARCH EXECUTIVE AGENCY (REA)

Department D

Data Protection Notice

Management of personal data in the context of REA Business Continuity Plan (BCP) – REA.D.2

In accordance with the Regulation (EU) 2018/1725 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[1] ('the Regulation'), the European Research Executive Agency ('the Agency' or 'REA') collects your personal information only to the extent necessary to fulfil a precise purpose related to our tasks.

1. WHY DO WE COLLECT YOUR PERSONAL DATA?

The REA Business Continuity Plan provides for arrangements to be implemented as a response to a crisis or unplanned disruptions of the Agency's activities. The processing is necessary to be able to rapidly inform staff on disruptions affecting the IT operations, the building or staff. It also allows for the crisis management team to activate the BCP and steer the recovery efforts, while keeping staff updated on the situation. For corporate events, the communication will be handled by SG or DG HR, depending on the nature of the crisis.

2. WHO IS RESPONSIBLE FOR THIS PROCESS?

The controller is the European Research Executive Agency (REA). For organisational reasons, the role of the data controller has been entrusted to Head of Department D (Coordination and Corporate Services).

You may contact the data controller via functional mailbox: REA-LSO@ec.europa.eu.

The processor is DG DIGIT and has extended rights as they have to manage NOAH for support and developments.

3. WHAT IS THE LEGAL BASIS TO COLLECT YOUR DATA?

Article 5(1) (a), (b), and (e) of the Regulation:

(a) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body2;

[1] 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 (OJ L 295 of 21.11.2018, p.39).

[2] **Council Regulation (EC) No 58/2003** of 19 December 2002 laying down the statute for executive agencies to be entrusted with certain tasks in the management of Community programmes, OJ L 11, 16.1.2003; **REA Establishment Act**: Commission Implementing Decision (EU) 2021/173 of 12 February 2021 establishing the European Climate, Infrastructure and Environment Executive Agency, the European Health and Digital Executive Agency, the European Research Executive Agency, the European Innovation Council and SMEs Executive Agency, the European Research Council Executive Agency, and the European Education and Culture Executive Agency and repealing Implementing Decisions 2013/801/EU, 2013/771/EU, 2013/778/EU,

(b) processing is necessary for compliance with a legal obligation to which the controller is subject;

(e) processing is necessary in order to protect the vital interests of the data subject or of another natural person (Article 5(1)(e) of Regulation);

The legal basis stems from art. 55 of Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Economic Community and the European Atomic Energy Community stating that "Officials in active employment shall at all times be at the disposal of their institution"; the Framework for Business Continuity Management in the Commission SEC(2006)898, Commission Staff Working Document SEC(2006)899; REA Internal Control Principle 10.4 (Business Continuity) and its subsequent local Business Continuity Plan.

4. WHICH PERSONAL DATA ARE COLLECTED?

Your personal data that is collected and processed in the context of this processing activity are the following:

♣ Identification and administrative data: First name, last name, unit, sector, office address

♣ Contact details: private mobile/smartphone number, private fixed phone number (optional), and private email address (optional)

♣ User data: log-in and function, date access and data changes/modifications (audit trail – each access and update/change is traced)

5. WHO WILL HAVE ACCESS TO YOUR PERSONAL DATA?

a. WHO WILL HAVE ACCESS TO THE DATA WITHIN THE AGENCY?

Access is always on a need-to-know basis and limited to the following authorised staff:

♣ Director;

♣ Business Continuity Correspondent;

♣ Heads of Department;

♣ Heads of Units, Heads of Sectors;

♣ Authorised agents;

♣ Local Security Officer

♣ BC Desk Officer;

♣ Duty officer.

2013/779/EU, 2013/776/EU and 2013/770/EU; and, **REA Delegation Act**: Commission Decision C(2021)952 of 12 February 2021 delegating powers to the European Research Executive Agency with a view to the performance of tasks linked to the implementation of Union programmes in the field of Research and Innovation, Research of the Fund for Coal and Steel and Information Provision and Promotion Measures concerning Agricultural Products comprising, in particular, implementation of appropriations entered in the general budget of the Union.

b. WHO WILL HAVE ACCESS TO THE DATA OUTSIDE THE AGENCY?

♣ Secretariat-General (SG) of the European Commission: In its corporate capacity and as NOAH system owner, the Secretariat-General can access all personal contact data (on need-to-know basis) for communication on corporate Business Continuity events (see DPR-EC-00583.3).

♣ Security Directorate of DG Human Resources (DG HR.DS): As responsible for corporate security, the Security Directorate at DG Human Resources can access all personal contact data (on need-to-know basis) for sending out messages to staff via the NOAH security module. For communication on security incidents, the primary tool is EUWARN (covered by DPR-EC-00826.3). Personal data processing in the context of security incidents is carried out by Commission staff members holding a valid security clearance up to level SECRET UE / EU SECRET and authorised to send security notifications. Access to relevant security communication tools is granted on a need-to-access basis and subject to user authentication and specific access rights.

♣ DG HR during a business continuity event may receive lists of staff affected by the incident.

♣ Office for Infrastructure Brussels (OIB) may receive lists for handling BC disruptions affecting offices of staff.

♣ DG DIGIT as system administrator.

In addition, data may be disclosed to public authorities, which are not regarded as recipient but may receive personal data in the frame of a particular inquiry in accordance with Union and Member State law, namely:

- The European Court of Justice or a national judge as well as the lawyers and the agents of the parties in case of a legal procedure;
- The competent Appointing Authority in case of a request or a complaint lodged under Articles 90 of the Staff Regulations;
- IDOC in line with Commission Decision of 12 June 2019 laying down general implementing provisions on the conduct of administrative inquiries and disciplinary proceedings - C(2019)4231
- OLAF in case of an investigation conducted in application of Regulation (EC) No 1073/1999
- The Internal Audit Service of the Commission within the scope of the tasks entrusted by article 118 of the Financial Regulation and by article 49 of the Regulation (EC) No 1653/2004
- The Court of Auditors within the tasks entrusted to it by Article 287 of the Treaty on the Functioning of the European Union of the EC Treaty and Article 20, paragraph 5 of Regulation (EC) No 58/2003
- The European Ombudsman within the scope of the tasks entrusted to it by Article 228 of the Treaty on the Functioning of the European Union
- The European Data Protection supervisor in accordance with Article 58 of the Regulation (EC) 2018/1725

- The European Public Prosecutor's Office within the scope of Article 4 of Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office

This transmission is restricted to the information necessary for the legitimate performance of tasks within the competence of the recipient. The recipients of the data are reminded of their obligation not to use the data received for other purposes than the one for which they were transmitted.

REA will not transfer your personal data to third countries (outside EU/EEA) or international organisations.

6. HOW LONG DO WE KEEP YOUR PERSONAL DATA?

The data items must be processed as long as the staff member is employed at the Agency. The start date of the processing is the start of service date, the end date is at the latest 3 months after date of end of service. This is the standard administrative time limit for ensuring handling of possible complaints.

For personal data in Business Continuity documents (BCP, telephone cascade, etc.) and annexes, they are kept as long as useful and up-to-date. The start date is the creation of the document and the end date is when the information is no longer useful and erased/updated.

NOAH-SYSPER sanity checks (automated discrepancy reports) are received on a monthly basis. Retention time is 6 months from date of email received (Outlook retention).

7. WHAT ARE YOUR RIGHTS?

At any time, you can access (online) your personal data under SYSPER2 and can rectify/erase the respective private information (mobile phone number (s), private phone number (fixed) and private email address or of a relative).

Any update in SYSPER2 will be reflected under NOAH the following day by 7 a.m.

You may also send your requests for change to REA HR (REA-HR@ec.europa.eu). In such a case, changes will be reflected in NOAH within 24 hours.

Any request from a data subject to exercise a right will be dealt within one month from receipt of the request. This period may be extended pursuant to Article 14(3) of Regulation (EU) 2018/1725.

Your right to information, access, rectification, erasure, restriction or objection to processing, communication of a personal data breach or due to confidentiality of electronic communications may be restricted only under certain specific conditions as set out in the applicable Restriction Decision in accordance with Article 25 of Regulation (EU) 2018/1725.

8. CONTACT INFORMATION

In case you have any questions about the collection/processing of your personal data, you may contact the data controller who is responsible for this processing activity by using the following email address: REA-LSO@ec.europa.eu.

Further to the above, the following instances can be addressed to:

REA Data Protection Officer (DPO): REA-DATA-PROTECTION-OFFICER@ec.europa.eu

In case of conflict, complaints can be addressed to the European Data Protection Supervisor: EDPS@edps.europa.eu.