EUROPEAN RESEARCH EXECUTIVE AGENCY (REA)

RECORD OF PERSONAL DATA PROCESSING ACTIVITY

In accordance with Article 31 of 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'), individuals whose personal data are processed by the European Research Executive Agency ('REA' or 'the Agency') in any context whatsoever are to be protected with regard to the processing of personal data and the Agency has to keep records of their processing activities.

Record No: 41
Created on (date): **10 July 2019**
Last update (date): **20 June 2022**

NAME OF THE PROCESSING ACTIVITY

Management of personal data in the context of the REA Business Continuity Plan (BCP)

GROUND FOR THE RECORD (TICK THE RELEVANT ONE):

☐ *Regularization of a data processing activity already carried out*
☐ *Record of a new data processing activity prior to its implementation*
☒ *Change of a data processing activity (e.g. update of a record)*

IDENTIFICATION OF THE DATA CONTROLLER

European Research Executive Agency (REA)

[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).

1. MANDATORY RECORD UNDER ARTICLE 31 OF THE REGULATION

(PART I - PUBLISHABLE VERSION FOR EXTERNAL PUBLICATION)

1.1. Contact details of controller

The controller is the European Research Executive Agency (REA), represented by its Director. For organisational reasons, the role of the data controller has been entrusted by the Director to the delegated controller and is exercised by Head of Department D – Coordination and Corporate Services. The data controller may be contacted via functional mailbox: *REA-LSO@ec.europa.eu*

1.2. Contact details of the Data Protection Officer (DPO)

REA DPO: REA-DATA-PROTECTION-OFFICER@ec.europa.eu

1.3. Name and contact details of joint controller (where applicable)

N/A

1.4. Name and contact details of processor (where applicable)

DG DIGIT: DIGIT-SYSPER2@ec.europa.eu)[2]

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 and/or OIB-55555@ec.europa.eu

1.5. Purpose of the processing

The REA Business Continuity Plan (BCP) provides for arrangements to be implemented as a response to a crisis or unplanned disruptions of the Agency's activities. The disruptions can affect the Agency's staff, operations or premises. Possible risks include fire, disabled access to the premises, serious IT failures, power cuts, pandemics, etc. The processing operation involving personal data is necessary in order to ensure that the members of the REA Crisis Management Team (CMT) are contacted/informed in due time, in case of a crisis, and for the activation/implementation of the "Telephone Cascade" process (part of the REA BCP), if the crisis situation would require so, for contacting the members of the REA staff. The members of the REA Crisis Management Team (CMT) are predominantly the Agency's managers, who have been appointed to perform certain critical functions in the context of the Business Continuity crisis management. Among others, the main role of the CMT is to activate REA's BCP, evaluate the nature and impact of the incident, decide on the immediate response actions and steer the recovery effort, prioritise activities to be maintained, decide on information/instructions to be communicated to staff, etc.

For corporate disruptions, the communication will be managed SG or DG HR, depending on the nature of the crisis. Personal data is collected through COMREF for NOAH BC tool and EU-Warn security tool. REA can access the NOAH tool to send SMS and/or e-mail to its staff. The purpose of these measures is not to intrude on staff's private lives. In normal circumstances the information would not be used and access to this information will be limited on a "need to know" principle to identified staff.

1.6. Legal basis for the processing

The processing is necessary for the performance of tasks carried out in the public interest or in the exercise of official authority vested in the Union institution or body (Article 5(1)(a) of Regulation).

[2] DG DIGIT has extended rights as they have to manage NOAH for support and developments.

The processing is necessary for compliance with a legal obligation to which the controller is subject (Article 5(1)(b) of Regulation).
The 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 specific legal basis:

♣ REA Business Continuity Plan (BCP) – (Revision dated February 2022);

♣ Council Regulation 58/2003 of 19 December 2002, laying down the Statute for executive agencies to be entrusted with certain tasks in the management of EU programmes;

♣ Regulation (EC) n° 1653/2004 of 21 September 2004 on a standard Financial Regulation for the executive agencies pursuant to Council Regulation (EC) n° 58/2003 of 19 December 2002 laying down the statute for executive agencies to be entrusted with certain tasks in the management of Community programme;

♣ Commission Implementing Decision (EU) 2021/173 of 12 February 2021 establishing the European Research Executive Agency, and repealing Implementing Decisions 2013/801/EU;

♣ 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 mobility, research and innovation;

♣ 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);

♣ Staff Regulations of Officials of the European Communities as fixed by regulation (CEE, Euratom, CECA) n° 259/68:

- Article 55 states that "Officials in active employment shall at all times be at the disposal of their institution"
- Conditions of employment of other servants of the European Communities: Article 16 and 91 states that the article 55 of the Staff Regulations shall apply by analogy.

This means that the Agency should have at its disposal information enabling it to contact its staff at all times. The obligation to provide home address details was confirmed many years ago by the Community courts and was expressed in general terms which make clear that the reasoning is transposable to more recent developments such as mobile phones numbers and private e-mail addresses. The subsequent data protection legislation has not amended the Staff Regulations in this respect and cannot justify any refusal to communicate such information to the employer.

1.7. Categories of data subjects

All REA staff (including external service providers, trainees and interim agents).

1.8. Categories of personal data

The 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)

1.9. Retention time (time limit for keeping the personal data)

Personal details are kept in NOAH for as long as the member of staff works at the REA plus 3 months administrative storage.

For personal data in Business Continuity documents (BCP, telephone cascade, etc) and annexes, they are kept as long as useful and up-to-date.

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).

Is any further processing for historical, statistical or scientific purposes envisaged? **No**

1.10. Recipients of the data

Who will have access to the data within the Agency?

♣ Director;

♣ Business Continuity Correspondent;

♣ Heads of Department;

♣ Heads of Units, Heads of Sectors;

♣ Authorised agents;

♣ Local Security Officer

♣ BC Desk Officer;

♣ Duty officer.

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.

1.11. Transfers of personal data to third countries or international organisations

No

1.12. High-level description of security measures

The contact details of the REA staff are stored in electronic format in databases and/or IT systems (Sysper2, NOAH) that reside on the servers of the European Commission. Storage of these full lists outside the database is only allowed for the Director and his back-up and authorised staff in unit D2 responsible for business continuity. A copy of the NOAH staff list is downloaded on a bi-monthly basis and stored on a usb and kept in a suitable safe for use if corporate databases are unavailable.

1.13. Data Protection Notice

A Data Protection Notice (DPN) relevant to this data processing is available in the REA public register of records and is transmitted by the data controller to the data subjects, where applicable.