EUROPEAN HEALTH AND DIGITAL EXECUTIVE AGENCY (HADEA)

RECORD OF PERSONAL DATA PROCESSING ACTIVITY

*In accordance with **Article 31 of the Regulation (EU) 2018/1725**[1] on the protection of natural persons with regards to the processing of personal data by the Union Institutions, bodies, offices and agencies and on the free movement of such data, 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.*

Therefore, each responsible HaDEA data controller has to maintain a record of the processing activities under his/her responsibility.

In accordance with Article 31 of the data protection regulation, 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:

Record No: - FIN - 01

Initial approval by Data Controller: n/a

Update (s) *(if applicable):*

NAME OF THE PROCESSING ACTIVITY

Ex-post audit

IDENTIFICATION OF THE DATA CONTROLLER

European Health and Digital Executive Agency (HaDEA), Head of Unit C2 Financial support and control

GROUND FOR THIS RECORD

□ Record of a new type of processing activity of personal data (before its implementation)

X **Record of a processing activity of personal data that is already in place**

□ Change/Amendment/ Update of an already existing previous record

[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 295/39 of 21.11.2018).

1. INFORMATION ON THE PROCESSING ACTIVITY

of Ex-post audits

This processing activity is performed in accordance with **Regulation (EU) No 2018/1725**[2] on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data.

1.1. The Data Controller is:

Head of Unit C2 "Financial support and control" in European Health and Digital Executive Agency (HaDEA), Place Charles Rogier 16, B-1049 Brussels, BELGIUM and can be contacted at HADEA-EXTERNAL-AUDITS@ec.europa.eu and HADEA-C2-SECRETARIAT@ec.europa.eu.

1.2. The contact details of the Data Protection Officer (DPO)

HADEA-DPO@ec.europa.eu

1.3. Joint controller:

Not applicable.

1.4. The following entities are acting as Processors:

In performance of the ex-post audits HaDEA uses external audit companies which are processing personal data as data processor when carrying the audits on behalf of HaDEA. Their names and contact details are available in data protection notice.

1.5. Description and purpose of this processing:

The ex-post audits of grant agreements and decisions aim at verifying beneficiaries' or subcontractors' or third parties' compliance with all contractual provisions (including financial provisions), in view of checking that the provisions of the grant agreement or decision were properly implemented and in view of assessing the legality and regularity of the transactions underlying the implementation of the Union budget.

Ex-post audits are mainly outsourced to external audit companies but could be carried out directly by HaDEA staff ("in-house audits").

[2] 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 295/39 of 21.11.2018).

1.6. The legal basis for the processing based on Article 5(1) of Regulation (EU) 2018/1725 is/are:

☒ **(a)** the 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 body[3] laid down in Union law;

☐ **(a2)** the processing is necessary for the **management and functioning** of the Union Institutions, bodies or agencies (Recital (22) of Regulation (EU) 2018/1725) laid down in Union law;

☒ **(b)** the processing is necessary for **compliance with a legal obligation** to which the controller is subject, which are laid down in Union law; [4]

☐ **(c)** the processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

☐ **(d)** the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;

☐ **(e)** the processing is necessary in order to protect the **vital interests** of the data subject or of another natural person.

[3] 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, 2013/779/EU, 2013/776/EU and 2013/770/EU. Commission Decision C(2021)948 final of 2 February 2021 delegating powers to the European Health and Digital Executive Agency with a view to the performance of tasks linked to the implementation of Union programmes in the field of EU4Health, Single Market, Research and Innovation, Digital Europe, Connecting Europe Facility – Digital, comprising, in particular, implementation of appropriations entered in the general budget of the Union. Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240. Regulation (EU) 2021/1153 of the European Parliament and of the Council of 7 July 2021 establishing the Connecting Europe Facility and repealing Regulations (EU) No 1316/2013 and (EU) No 283/2014. Regulation (EU) 2021/522 of the European Parliament and of the Council of 24 March 2021 establishing a Programme for the Union's action in the field of health ('EU4Health Programme') for the period 2021-2027, and repealing Regulation (EU) No 282/2014. Regulation (EU) 2021/690 of the European Parliament and of the Council of 28 April 2021 establishing a programme for the internal market, competitiveness of enterprises, including small and medium-sized enterprises, the area of plants, animals, food and feed, and European statistics (Single Market Programme) and repealing Regulations (EU) No 99/2013, (EU) No 1287/2013, (EU) No 254/2014 and (EU) No 652/2014.

[4] Article 74(6) of Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union. Commission Decision C(2021)948 final of 2 February 2021 delegating powers to the European Health and Digital Executive Agency with a view to the performance of tasks linked to the implementation of Union programmes in the field of EU4Health, Single Market, Research and Innovation, Digital Europe, Connecting Europe Facility – Digital, comprising, in particular, implementation of appropriations entered in the general budget of the Union. Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240. Regulation (EU) 2021/1153 of the European Parliament and of the Council of 7 July 2021 establishing the Connecting Europe Facility and repealing Regulations (EU) No 1316/2013 and (EU) No 283/2014. Regulation (EU) 2021/522 of the European Parliament and of the Council of 24 March 2021 establishing a Programme for the Union's action in the field of health ('EU4Health Programme') for the period 2021-2027, and repealing Regulation (EU) No 282/2014. Regulation (EU) 2021/690 of the European Parliament and of the Council of 28 April 2021 establishing a programme for the internal market, competitiveness of enterprises, including small and medium-sized enterprises, the area of plants, animals, food and feed, and European statistics (Single Market Programme) and repealing Regulations (EU) No 99/2013, (EU) No 1287/2013, (EU) No 254/2014 and (EU) No 652/2014. The right to carry out audits is foreseen in the agreements with the beneficiaries.

1.7 The categories of data subjects

- ☐ Agency staff (Contractual and temporary staff in active position)
- ☐ Visitors to the Agency
- ☐ Applicants
- ☐ Relatives of the data subject
- ☐ Complainants, correspondents and enquirers
- ☐ Witnesses
- ☒ Beneficiaries
- ☐ External experts
- ☐ Contractors
- ☒ Other, please specify: Staff members and subcontractors of beneficiaries or any other natural persons involved in the matter being audited.

1.8 Categories of personal data

a) Categories of personal data:

- Identification such as first and last name, staff number, title, function, grade, contact details (phone number, personal and professional address, email address, communications) etc.
- Data concerning the data subjects' career such as: professional activities and expertise, CV etc.
- Data subject's family names and contact details (email addresses, personal and professional address, telephone numbers and communications).
- Financial data such as invoices, salaries, pay slips as well as relevant information such as performed hours linked to named staff/ staff number, timesheets, information about leave and absences, social security and pensions, expenses and medical benefits, individual hourly rate calculation, employment contracts, accounting records (including Payroll), cost accounting, information coming from local IT system used to declare costs, bank accounts etc.
- Supporting documents substantiating the expenses of the project such as minutes of meetings/ events, mission reports, travel costs etc.

This list of data requested is indicative, without prejudice for the Agency and its contractors to ask any other relevant information as foreseen under the relevant Articles of the grant agreements. Only personal data, which is necessary for the processing operation in the light of its purpose will be used.

b) Categories of personal data processing likely to present specific risks:

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): processing of such data is purely incidental but might take place in case of exclusion as provided for by Financial Regulation.

c) Categories of personal data whose processing is <u>prohibited</u>, with exceptions (art. 10):

Auditors might have access to such data[5] but they are disregarded as they are not in the scope of their audit.

d) Specify any additional data or explanatory information on the data being processed, if any:

Audit team in C.2.002 keeps two categories of data, i.e. a) project data (e.g. project number and type, global budget, etc.) and b) data of beneficiary (such as address of the organisation, name, contact details of the persons responsible for the projects, personal data linked to audit findings). The categories of data contained in documents may vary depending on the nature of the project and the matter being audited.

1.9 Retention period (maximum time limit for keeping the personal data)

The personal data concerned **will be kept for a maximum period** of 10 years[6] from the closure of the annual audit plan file where audit information is stored. On condition that no contentious issues occurred; in this case, data will be kept until the end of the last possible legal procedure.

Data will be manually deleted at the end of this period.

Is any further processing for historical, statistical or scientific purposes envisaged?

☐ yes ☒ no

1.10 The recipients of the data

The recipients to whom the personal data will or might be disclosed are:

Within the Agency:

- Designated staff of HaDEA such as:
  - financial/project/legal officers in HaDEA;
  - Audit Liaison Officers in HaDEA;
  - Authorised Officers by (sub-) Delegation in HaDEA (Director, Heads of Department, Heads of Unit, Heads of sector);

5 E.g. data revealing ethnic or racial origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data for identification purposes, data concerning health or sex life or sexual orientation, criminal convictions or offences and related security measures or otherwise considered sensitive.

6 The retention period should be decided in accordance with the Commission's common retention list.

- HaDEA's Internal Controller, Data Protection Officer, Legal Affairs Sector, etc.

Outside the Agency:

- External auditors (processors) acting on behalf of HaDEA, and their subcontractors if any;
- European Commission staff, such as DGs, Commission services in charge of ex-ante or ex-post controls and the implementation of audit results;
- Joint Undertakings (JUs)[7] and the European Cybersecurity Industrial, Technology & Research Competence Centre (ECCC), implementing Digital Europe Programme and in charge of ex-post controls and the implementation of ex-post audit results in relation to their grant agreements and decisions.

In addition, in case of control or dispute, personal data can be shared with and processed by the bodies charged with a monitoring or inspection task in application of Union law in compliance with the applicable data protection rules and within the scope of their tasks entrusted by the relevant legislation. This includes, in particular, the following recipients:

- Bodies in charge of a monitoring or an inspection task in application of Union law (e.g. internal audit, IAS, Court of Auditors, etc.);
- 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;
- OLAF in case of an investigation conducted in application of Regulation (EC) No 1073/1999;
- 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 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.

1.11 Transfers of personal data to third countries or international organisations

Your personal data **might be transferred** to the following third countries: the United Kingdom in case one of our contractors which is based in the United Kingdom will perform the audit on HaDEA's behalf. In such case the transfer takes places on the basis of an adequacy decision.[8]

---

[7] Two Joint Undertakings - The European High Performance Computing Joint Undertaking (EuroHPC JU) and Chips Joint Undertaking (Chips JU). The JUs are independent legal entities based on Article 187 of the Treaty on the Functioning of the European Union (TFEU). HaDEA is responsible for ex-post controls of the Digital Europe Programme for the whole programme (Annex I of Commission Decision C(2021)948 final).

[8] Commission Implementing Decision of 28.6.2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom C(2021) 4800.

1.12 The processing of this personal data **will not include** automated decision-making (such as profiling).

1.13 Description of security measures

The following technical and organisational security measures are in place to safeguard the processing of this personal data:

The European Commission's IT systems used by the Agency abide by the Commission's security guidelines. The Agency complies with Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission.

1. Organisational measures:

A Corporate Local Informatics Security Officer (C-LISO) is in place. Its role includes supervising the Agency compliance with the relevant regulations, and the application of security measures recommend by DIGIT.

Organisational measures include appropriate access rights and access control. As a rule within the Agency, access to information systems, the file system or offices are subject to a series of authorisations where the person granting the access is different from the person requesting or authorising the access - except in limited cases of delegation. The responsible person in the unit in charge of this action (processing operation of the current record) collects and places personal data in electronic format on the secured drive of the Unit with restricted access on a need to know basis. All Agency staff and its contractors are bound by confidentiality obligations. The need to know principle applies in all cases.

2. Technical measures

State of the art technical cybersecurity measures are implemented in the corporate systems, according to the security needs. Those measures are in constant evolution.

1.14 Data protection Notice

Data Subjects are informed on the processing of their personal data via a **data protection notice on their rights:**

- to access their personal data held by a controller;
- to request their personal data held by a controller to be corrected;
- to obtain in some situations erasure of their personal data held by a controller, e.g. when data are held unlawfully (right to be forgotten);
- to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- **of recourse** at any time to the **HaDEA Data Protection Officer** at HADEA-DPO@ec.europa.eu and to the **European Data Protection Supervisor** at https://edps.europa.eu.

Request from a data subject to exercise a right will be dealt within **one month**.

Your right to information, access, rectification, erasure, restriction or objection to processing, communication of a personal data breach or 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.