



## **Data Protection Notice for the Management of personal data in the context of the HaDEA Business Continuity Plan (BCP)**

The European Health and Digital Executive Agency (HaDEA) processes your personal data<sup>1</sup> in line with [Regulation \(EU\) 2018/1725 of the European Parliament and of the Council of 23 October 2018<sup>2</sup>](#) on the protection of personal data by the European Union's institutions, bodies and agencies and on the free movement of such data.

### **WHAT IS THE PURPOSE(S) OF THIS PROCESSING ACTIVITY?**

The HaDEA 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 BCP is in place to ensure that the Agency is able to continue its operation to the extent possible in case of a disruption.

Within the business continuity framework, the purpose of the processing of personal data is to enable the Agency, if the situation of disruption would require so, to contact each HaDEA staff member where necessary in view to:

- ensure the staff members security and safety;
- safeguard continuity of service and to prevent major disruptions of its activities;
- prepare exercises and respond to crises and operational disruptions affecting the normal functioning of the Agency;
- accelerate the exchange of information and distribution of instructions on actions to be taken in the interests of the staff and HaDEA.

Processing of personal data may occur through the use of a communication/phone channels, for example through the use of Private Messenger(s)<sup>3</sup> or through the use of NOAH tool. Specific

<sup>1</sup> Personal data shall mean any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

<sup>2</sup> 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 L295/39 of 21.11.2018).

<sup>3</sup> Private Messenger, (e.g. Signal Private Messenger), is a mobile application designed to send and receive messages and voice/video calls that are highly secured and always end-to-end encrypted so they can never be shared or viewed by anyone but yourself and the intended recipients. No third party, including the Private Messenger, has the ability to decrypt or otherwise access the content of your calls or messages. Private Messenger does not store your message history. Any storage of additional technical information is limited to the minimum required for its operation. Any sharing of your data by Private Messenger must be legally justified by the special circumstances clearly stated in its official

information on the processing of data via the NOAH tool can be found in the EC record at this link: <https://ec.europa.eu/dpo-register/detail/DPR-EC-00538>). These processing activities enable the Agency to safeguard continuity of service and to warn staff about situations that could be prejudicial to their safety or security.

#### **WHO IS THE DATA CONTROLLER?**

The data controller of the processing operation is the Head of Department Finance and Resources of the European Health and Digital Executive Agency (HaDEA).

#### **WHICH PERSONAL DATA IS COLLECTED?**

The mandatory personal data collected and processed for the purposes outlined above is the following: name, surname, private mobile number and service mobile number (if relevant).

The selected Private Messenger application can collect: private and/or service phone number used for registration into the application, date of account creation and the date of last use. All other information shall be optional and end-to-end encrypted.

The data will be collected through Sysper, NOAH and where necessary directly from staff.

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.

#### **WHO HAS ACCESS TO THE PERSONAL DATA OF DATA SUBJECTS AND TO WHOM CAN THEY BE DISCLOSED?**

The recipients of your personal data, on a need to know basis, are:

- The members of the Crisis Management Team (CMT) composed by the Director, the Heads of Department, the Head of Unit C3 Staff, Communication and Support, the BC Desk Officer and the Duty Officers and where necessary other staff members that participate to CMT meetings (e.g. staff charged with filtering and passing of communication; administrative and secretarial tasks; arranging logistics, etc.).
- Bodies charged with monitoring or inspection tasks in application of EU law or national law (e.g. internal audits, Court of Auditors, European Anti-fraud Office (OLAF), the European Public Prosecutor Officer (EPPO), the European Ombudsman, the European Data Protection Supervisor).
- On a need to know basis the following services of the European Commission: Security Directorate of DG Human Resources as responsible for corporate security, for sending out security messages to staff; the Secretariat General (as system owner of the NOAH tool); DG DIGIT (as system administrator of NOAH), OIB (e.g. for the management of access to buildings).

Your personal data **will not be transferred** to third countries or international organisations.

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

The relevant content of the communication in the Private Messenger application will be held by the intended recipients. The intended recipients are responsible for taking appropriate precautions to ensure the physical security of the data support and to prevent any unauthorized disclosure or access.

Terms and policies (e.g. protection the national or public security, prevent, investigate, detect and prosecute of criminal offences or otherwise address fraud and to protect from harm to the rights, property, or safety of the Private Messenger and its users)

The recipients to whom the collected personal data will or might be disclosed by the Private Messenger are defined in the specific Terms and Privacy policies of the selected mobile application (e.g. Signal)<sup>4</sup>.

The use of a Private Messengers being a third party IT tool does not in any way imply that HaDEA endorses them or their privacy policies. In the event that one or more third party IT tools are occasionally unavailable, HaDEA holds no responsibility for lack of service due to their downtime.

## **WHAT IS THE LEGAL BASIS TO COLLECT YOUR DATA?**

The legal basis applying to this processing operation are:

- Article 5(1)(a) of the Data Protection Regulation given that 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;
- Article 5(1)(b) given that the processing is necessary for compliance with a legal obligation to which the controller is subject;
- Article 5(1)(e) processing is necessary in order to protect the vital interests of the data subject or of another natural person.

### **Specific legal basis:**

- 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 (OJ L 50/9 of 15.2.2021);
- Articles 55 of the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Economic Community and the European Atomic Energy Community;
- HaDEA Business Continuity Plan;
- Framework for Business Continuity Management in the Commission: Communication to the Commission SEC(2006)898;
- Commission Staff Working Document Framework for business continuity management in the Commission SEC(2006)899;
- Internal Control Framework: Principle 10 “Select and Develop control activities”;

## **HOW LONG DO WE KEEP YOUR PERSONAL DATA?**

Personal details are kept for as long as the person works in HaDEA or provides a service in the HaDEA plus three months for smooth service operation. Data will be automatically deleted at the end of your assignment in HaDEA and/or upon your request.

For the data collected through NOAH tool please refer to the specific EC Record at the following link: <https://ec.europa.eu/dpo-register/detail/DPR-EC-00538>.

<sup>4</sup> <https://signal.org/legal/#terms-of-service>

## **WHAT ARE YOUR RIGHTS REGARDING YOUR PERSONAL DATA?**

You have the right to access your personal data and to request your personal data to be rectified, if the data is inaccurate or incomplete; where applicable, you have the right to request restriction or to object to processing, to request a copy or erasure of your personal data held by the data controller.

If processing is based on your consent, you have the right to withdraw your consent at any time, without affecting the lawfulness of the processing based on your consent before its withdrawal.

Your request to exercise one of the above rights will be dealt with without undue delay and within **one month**.

If you have **any queries** concerning the processing of your personal data or wish to exercise any of the rights described above, you can contact the Head of Department C Finance and Resources (entity acting as data controller) via: [HADEA-BCP@ec.europa.eu](mailto:HADEA-BCP@ec.europa.eu) and HaDEA DPO [HADEA-DPO@ec.europa.eu](mailto:HADEA-DPO@ec.europa.eu)

**You shall have right** of recourse at any time to the European Data Protection Supervisor at [EDPS@edps.europa.eu](mailto:EDPS@edps.europa.eu).

Version [*February – 2022, revision 1.0*]