EUROPEAN EDUCATION AND CULTURE
EXECUTIVE AGENCY (EACEA)

RECORD OF PERSONAL DATA PROCESSING

Art. 31 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 (henceforth the "Regulation")

Record n° *2021 / 04*

In accordance with Article 31 of Regulation 2018/1725, individuals whose personal data are processed by 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 operations.

This record covers two aspects:

1. Mandatory records under Art 31 of the 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.*

EACEA- Business Continuity Management	
1	**Last update of this record (where applicable)**
	N/A
2	**Short description of the processing**
	Processing names, phone numbers and other contact details in order to ensure business continuity in case of crises and operational disruptions outside the data processed in NOAH. (For data processed in NOAH, see DPR-EC-00538.3.)
Part 1 - Article 31 Record	
3	**Name of the Controller** **Unit(s) and/or function of person acting on behalf of the Controller**

	Controller: European Education and Culture Executive Agency Unit: R1 – People, Workplace and Communication e-mail: EACEA-HR@ec.europa.eu
4	**Contact details of the Data Protection Officer (DPO)**
	EACEA-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)**
	N/A
7	**Purpose of the processing**
	EACEA collects and uses personal information to enable the Agency to respond to crises and operational disruptions affecting the normal functioning of the institution by using the personal contact details of staff for communication purposes. Business Continuity Management helps the EACEA to prepare and respond to business disruptions in the event of a crisis. **The processing is necessary to**: • Ensure the staff members security and safety; • Enable the EACEA to 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 EACEA The Business Continuity Plan should provide management and staff with a pragmatic, user-friendly, guide to the measures EACEA has put in place in order to respond to crises and to ensure continued delivery of its essential tasks. **The processing of personal data is necessary for the management and the functioning of the EACEA**. It is based on Staff Regulations and the Business Continuity Management Framework (SEC(2006)899) as it is in the interests of both the institution and staff. **It enables the EACEA to ensure continuity of service and to send information to staff**. Under this record, staff personal contact details shall be processed and used exclusively for business continuity management purposes, i.e. to prepare exercises and respond to crises and operational disruptions affecting the normal functioning of the EACEA.
8	**Description of the categories of data subjects**
	Whose personal data are being processed? In case data categories differ between different categories of persons, please explain as well (e.g. suspects vs. witnesses in administrative inquiries) ☒ Agency staff (Contractual and temporary staff in active position) ☐ Visitors to the Agency ☐ Contractors providing goods or services

	☐ Applicants ☐ Relatives of the data subject ☐ Complainants, correspondents and enquirers ☐ Witnesses ☐ Beneficiaries ☐ External experts ☐ Contractors ☒ Other, please specify: External service providers and interim staff
9	**Description of personal data categories**
	Indicate <u>all</u> the categories of personal data processed and specify which personal data are being processed for each category (between brackets under/next to each category): ***a) Categories of personal data:*** ☐ in the form of personal identification numbers ☐ concerning the physical characteristics of persons as well as the image, voice or fingerprints ☒ concerning the data subject's private sphere **(name and surname)** ☐ concerning pay, allowances and bank accounts ☐ concerning recruitment and contracts ☐ concerning the data subject's family ☐ concerning the data subject's career ☐ concerning leave and absences ☐ concerning missions and journeys ☐ concerning social security and pensions ☐ concerning expenses and medical benefits ☒ concerning telephone numbers and communication**s (private telephone numbers)** ☒ concerning names and addresses (including email addresses) **(private e-mail addresses, personal addresses)** ☒ Other: please specify: **user login, user function and date of login and information on changes in NOAH (N.B. NOAH implements an "audit trail" technique tracking each access and handling of personal data in NOAH to trace back all accesses and changes.** ***b) Categories of personal data processing likely to present <u>specific risks:</u>*** ☐ 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) ***c) Categories of personal data whose processing is <u>prohibited</u>, with exceptions (art. 10):*** ☐ revealing racial or ethnic origin

☐ revealing political opinions

☐ revealing religious or philosophical beliefs

☐ revealing trade-union membership

☐ concerning health

☐ genetic data, biometric data for the purpose of uniquely identifying a natural person

☐ concerning sex life or sexual orientation

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

10 **Retention time (time limit for keeping the personal data)**

EACEA only keeps your personal data for the time necessary to fulfil the purpose of collection or further processing, namely:

Category	Retention period	Start date	End date
all personal data are kept by the Commission in the NOAH database	personal details of staff are kept for the duration of active employment in the EACEA	recruitment	3 months after the date of retirement or end of service
automatic and manually extracted reports from NOAH IT tool: a) Extracted by DG HR and sent to EACEA: (via BC Desk Officer/BC Contact Point) receives monthly/weekly "NOAH - SYSPER sanity check" automatic reports indicating any discrepancies in Sysper data (missing phone numbers). b) Any NOAH user can extract customized reports c) DIGIT can access to the list of critical and essential staff (incl. full name of staff and their office number), which is automatically synchronized with their system management tool during a crisis.	6 months	a), and d) date of email received b), and c) date of extraction	a) and d) 6 months from date of email received b), and c) 6 months from date of extraction

	d) OIB and DG HR may receive a list of critical and essential staff (incl. full name of staff and their office number) extracted from NOAH during any business continuity event.			
	Business Continuity Plan and annexes	5 years	creation of document	5 years

Is any further processing for historical, statistical or scientific purposes envisaged?
☐ yes ☒ no

If yes, indicate the further retention time:

If the answer is yes, please go to Part 2, Storage and Security for technical safeguards.

11 **Recipients of the data**

As for the Business Continuity Plan and annexes, they are published on EACEA's Intranet and thus available to all Agency staff. The Annexes include a list with names of CEN (Critical, Essential and Necessary).

The contact details of CEN staff are also available to Members of Business Continuity Management Team (CMT), line managers, the head of HR sector and their back up.

The CMT is composed of:

- ✓ Director of the Agency
- ✓ Director's assistants
- ✓ Head of Unit from Unit R1 to provide expertise on all administrative matters.
- ✓ Head of Unit from Unit R2 to provide expertise on financial resources.
- ✓ Head of Unit from Unit B6 to provide expertise on IT and logistical matters.
- ✓ Head of Sector from Unit R1, LSO and Duty Officer to provide expertise on Logistics and Security matters.
- ✓ Head of Sector from Unit R1-RH to provide expertise on Human Resources.
- ✓ Head of Sector from Unit R1-COMM to provide expertise on Communication.

The list with names of duty officers is published on EACEA's Intranet and thus available to all Agency staff. Their contact details are available just to the members of CMT, line managers, the head of HR sector and their back up.

12 **Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?**

No.

13 **General description of the technical and organisational security measures**

1. Organisational measures:

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 HR

	responsible person collects and places the documents either in a confidential file which is kept under locks in the HR offices accessible only to designated HR staff on a need-to-know basis or in the staff personal files, which are kept under locks accessible only to designated HR staff on a need-to-know basis. **2. Technical measures:** Technical measures include the use of secure equipment. The Agency's IT systems abide by the Commission's security guidelines. The Agency must comply with Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission. In this context a specific 'Information Security Technology Plan' is reviewed annually with a view to describe the implementation of the above rules and guidelines in EACEA. The procedures set out in the document must be applied to the Agency's IT systems to ensure the security of the stored data and they are based on the European Commission's standards on security. The Server Rooms of the Agency are equally protected and locked.
14	**Information to data subjects / Privacy Statement**
	A privacy statement concerning data processing related to the Business Continuity Plan outside NOAH is published on the Agency's intranet.