



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°

001-2020

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.

Personal files of staff members	
1	Last update of this record (where applicable) The last version of this record was from March 2020 (reference n° 001-2020).
2	Short description of the processing One of the main assignments of the HR Unit R1 of EACEA (hereinafter referred to as "HR") is to manage and to implement Human Resources policies and procedures in the

	<p>Agency. This includes the management of staff personal data, collected in the personal files (Paper and electronic in SYSPER).</p> <p>SYSPER is the corporate information system supporting Human Resources Management processes from recruitment to retirement. Over the years, SYSPER has integrated several HR business processes like time management, appraisal and promotion etc. Since 2014 the Agency has access to the Module “Personal files” through the NDP (“Numérisation des Dossiers Personnels”) -Personal files tool and the Agency digitalised all paper personal files that since 2016 can be consulted by staff members directly in SYSPER.</p>
Part 1 - Article 31 Record	
3	<p>Name of the Controller Unit(s) and/or function of person acting on behalf of the Controller</p> <p>Controller: European Education and Culture Executive Agency</p> <p>Unit(s): Unit R1 – People, Workplace and Communication EACEA-PERSONAL-FILES@ec.europa.eu</p>
4	<p>Contact details of the Data Protection Officer (DPO)</p> <p>EACEA-data-protection@ec.europa.eu</p>
5	<p>Name and contact details of joint controller (where applicable)</p> <p>N/A</p>
6	<p>Name and contact details of processor (where applicable)</p> <p>DG HR owner of SYSPER AND NDP IT TOOL</p> <p>Service Level Agreement between DG HR and EACEA (Ares(2017)6026178 and Ares(2021)7445821- Amendment 3)</p>
7	<p>Purpose of the processing</p> <p>The purposes of this operation are the following:</p> <ul style="list-style-type: none"> – to support the management of rights, obligations and career matters of all staff members (from entry into service up to end of service); – to centralise the information; – to enable active and retired personnel to exercise their rights (e.g., allowances); – to better secure the physical management of files and to improve their accessibility (staff and authorised person or service); – to ensure the confidentiality of information contained in the personal file.
8	Description of the categories of data subjects

	<input checked="" type="checkbox"/> Agency staff (Contractual and temporary staff in active position) <input type="checkbox"/> Visitors to the Agency <input type="checkbox"/> Contractors providing goods or services <input type="checkbox"/> Applicants <input checked="" type="checkbox"/> Relatives of the data subject <u>children, spouses, other dependant members</u> <input type="checkbox"/> Complainants, correspondents and enquirers <input type="checkbox"/> Witnesses <input type="checkbox"/> Beneficiaries <input type="checkbox"/> External experts <input type="checkbox"/> Contractors <input checked="" type="checkbox"/> Other: retired agency staff (Contractual and temporary agents)
9	Description of personal data categories
	<p><i>a) Categories of personal data included in Personal Files:</i></p> <input checked="" type="checkbox"/> in the form of personal identification numbers personal perID number, personal number, NUP <input type="checkbox"/> concerning the physical characteristics of persons as well as the image, voice or fingerprints <input checked="" type="checkbox"/> concerning the data subject's private sphere <ul style="list-style-type: none"> - date of birth, - place of birth, - place of origin, - gender, - nationality, - standard form replacing the criminal record, - military service, - civil status certificate, - the countries of previous residence <input checked="" type="checkbox"/> concerning pay, allowances and bank accounts <ul style="list-style-type: none"> - information on the employment status of a spouse, - information on the number of children and other dependant member, - place of origin, - place of residence, - bank accounts details (BAF) and legal entity <input checked="" type="checkbox"/> concerning recruitment and contracts <ul style="list-style-type: none"> - application form, - CV, - diplomas, information on the education, - professional experience with recommendations/confirmations, - offer letter and offer acceptance, - contract(s), - medical aptitude (pre-employment visit) – the document only specifies that “the person is apt for work”.

<input checked="" type="checkbox"/> concerning the data subject's family <ul style="list-style-type: none"> - personal details of a spouse, - matrimonial- divorce certificate, - number of children, - children and/or other dependant member name, birth date, education (school attended, university), personal details of other parent, - children birth certificate, - place of residence of parents <input checked="" type="checkbox"/> concerning the data subject's career <ul style="list-style-type: none"> - information on previous work experiences, - declaration of the acceptance of rights and obligations <input checked="" type="checkbox"/> concerning leave and absences <ul style="list-style-type: none"> - CCP (Congé de convenance personnelle) <input type="checkbox"/> concerning missions and journeys <input checked="" type="checkbox"/> concerning social security and pensions <ul style="list-style-type: none"> - legal entity, - financial identification, - determination of rights and receipts (PMO forms), - allowances (child, household, education, installation/removal, expatriation, daily), - pension, - checklist in case of departure/ termination of the contract, - travel costs on taking up the duty, - allowances from the other/external source <input type="checkbox"/> concerning expenses and medical benefits <input type="checkbox"/> concerning telephone numbers and communications <input checked="" type="checkbox"/> concerning names and addresses (including email addresses) <ul style="list-style-type: none"> - name, surname, contact details, address, permanent address <input type="checkbox"/> Other: languages, additional skills, IT & office skills, copy of passport or ID card <p><i>b) Categories of personal data processing likely to present <u>specific risks</u>:</i></p> <input type="checkbox"/> data relating to suspected offences, offences, criminal convictions or security measures <input checked="" type="checkbox"/> data being used to evaluate personal aspects of the data subject (ability, efficiency, conduct) <ul style="list-style-type: none"> - probationary report, - appraisal reports, - reclassification, - disciplinary affairs (final decisions) <p><i>c) Categories of personal data whose processing is <u>prohibited</u>, with exceptions (art. 10):</i></p> <input type="checkbox"/> revealing racial or ethnic origin <input type="checkbox"/> revealing political opinions <input type="checkbox"/> revealing religious or philosophical beliefs <input type="checkbox"/> revealing trade-union membership <input type="checkbox"/> concerning health

	<input type="checkbox"/> genetic data, biometric data for the purpose of uniquely identifying a natural person <input type="checkbox"/> concerning sex life or sexual orientation <i>d) Specify any additional data or explanatory information on the data being processed, if any: -----</i>
10	<p>Retention time (time limit for keeping the personal data)</p> <p>Retention time for personal files is 8 years after the extinction of all rights of the person concerned and of any dependants, and for at least 100 years after the recruitment of the person concerned (12.3.7 of CRL). Afterwards files are eliminated.</p> <p><u>Exceptions:</u></p> <p>Disciplinary procedures A staff member may, after 3 years (in the case of a written warning or reprimand) or after 6 years (in the case of any other penalty) submit a request for the deletion from his personal file of all reference to such measure. If the request is granted, the decision is eliminated</p> <p>Is any further processing for historical, statistical, or scientific purposes envisaged? <input type="checkbox"/> yes <input checked="" type="checkbox"/> no</p>
11	<p>Recipients of the data</p> <ul style="list-style-type: none"> • R1 HR Unit EACEA designated staff • Director EACEA • DG HR or another European Institution (in case of inter-institutional transfer of the staff member) • DG DIGIT (provides technical support for Sysper). • DG DIGIT (system supplier of NDP). • The Pay Master Office (PMO), in their specific field of competence <p>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:</p> <ul style="list-style-type: none"> • 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 European Anti-Fraud Office (OLAF); • The Internal Audit Service of the Commission • The Investigation and Disciplinary Office of the Commission (IDOC) • The European Court of Auditors • The European Ombudsman • The European Public Prosecutor's Office • EU courts and national authorities
12	<p>Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?</p> <p><u>N/A</u></p>
13	<p>General description of the technical and organisational security measures</p>

	<p>The European Commission's IT systems used by the Agency 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.</p> <p><u>1. Organisational measures</u></p> <p>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.</p> <p>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 the documents on the secured drives of the Commission and all Agency staff are bound by a confidentiality obligation. The need to know principle applies in all cases.</p> <p>The paper personal files are kept in a secured archive, securely locked up. Only designated HR staff have access to the files on a know-to-know basis.</p> <p>Only designated HR staff has access to the Agency personal files SYSPER in the NDP tool.</p> <p>Each staff member has access to the electronic version of his/her personal file in SYSPER (ECAS password).</p> <p><u>2. Technical measures:</u></p> <p>State of the art technical cybersecurity measures are implemented in the corporate systems, according to the security needs. Those measures are in constant evolution.</p> <p>SYSPER system is constructed and maintained in the manner described in the Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission.</p> <p>The paper version of the documentation is stored in locked cupboards and then in the archives in a locked room.</p>
14	<p>Information to data subjects / Privacy Statement</p> <p>A specific privacy statement is available on the EACEA intranet page (Personal File (europa.eu))</p> <p>The SYSPER privacy statements as well a more specific information on personal file are made available to staff by the Commission on MyIntraComm.</p>