EUROPEAN COMMISSION
European Education, and Culture Executive Agency

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 nº	09-2022

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.*

APPFIN/ PEGASUS I and II: management of financial transactions and configuration	
1	**Last update of this record (where applicable)**
	Not applicable
2	**Short description of the processing**
	APPFIN and Pegasus are management tools with an IN/OUT interface to the ABAC system (interrupted since the obsolescence of ABAC, as from 01/01/2025), used for the legacy projects (before MFF 2021-2027). It is used by the services for the automatic creation of financial transactions (budgetary and legal commitments, payments/reimbursements and 'third party' forms) in the context of grants and procurements.. The relevant contracts are automatically generated by APPFIN and PEGASUS, as well. Unit R2 grants access to APPFIN and PEGASUS to designated staff member from the the operational units of the Agency, who has a special authorization of the Head of Units.

	Various levels of access are defined by Unit R2 in the system, corresponding to functions determined in the financial process: operational initiator, financial initiator, financial verifier and operational verifer. A system of sequential visa allows a level of control for the creation/validation of the financial files, registering the debits and credits.

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 Head of unit R2 for APPFIN (System owner) Head of unit A1 for PEGASUS (System owner) Contact details are: APPFIN and Pegasus 2 (section monitoring): EACEA-APPFIN@ec.europa.euPegasus 1 and Pegasus 2 (section selection): EACEA-HELPDESK@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)**
	NA
6	**Name and contact details of processor (where applicable)**
	N/A
7	**Purpose of the processing**
	The use of both systems is necessary for the prompt and efficient management of financial transactions in the framework of EU programmes, in compliance with the Financial Regulation. In particular, the use of the system enables the automatic generation of: - contracts; - commitments; - payments; - recovery orders; - de-commitments. Various levels of access are defined in the system, corresponding to functions determined in the financial process: operational initiator, financial initiator, financial verifier and operational verifier. Access rights to Pegasus are managed through PMTAC.
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:
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 ☒ concerning pay, allowances and bank accounts of beneficiaries, and contractors ☐ concerning recruitment and contracts ☐ concerning the data subject's family ☒ concerning the data subject's career (contract duration of staff) ☐ concerning leave and absences ☐ concerning missions and journeys ☐ concerning social security and pensions ☐ concerning expenses and medical benefits ☒ concerning telephone numbers and communications ☒ concerning names and professional email addresses ☐ Other: please specify: _____ ***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)**
	Indicate the period of storage: For grants and procurements: retention period for rejected applications are kept for 5 years, and 10 years after final payement for beneficiaries. Personal data for access rights of staff in APPFIN: for the duration of existence of the appliance. Personal data for access rights of staff to PEGASUS: for the duration of existence of the appliance. **Is any further processing for historical, statistical or scientific purposes envisaged?** ☐ yes ☒ no **If yes, indicate the further retention time:**
11	**Recipients of the data**
	Access to personal data is granted on a need to know basis to the Agency staff dealing with the financial transactions and projects management. In addition, data may be disclosed to public authorities, and processed by these authorities in compliance with the applicable data protection rules according to the purpose of the processing, including inter alia: □ 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; □ 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; □ 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 and Commission Decision (EU) 2019/165 of 1 February 2019 Internal rules concerning the provision of information to data subjects and the restriction of certain of their data protections rights in the context of administrative inquiries, pre-disciplinary, disciplinary and suspension proceedings; □ 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 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.
12	**Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?**
	Not Applicable
13	**General description of the technical and organisational security measures**
	Include a general description of your technical and organisational security measures that you could also provide to the data subjects and general public. 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. 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 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. 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.
14	**Information to data subjects / Privacy Statement**
	Privacy statement will be published on the website (https://www.eacea.ec.europa.eu/about-eacea/data-protection_en) of the Agency and on the Intranet (https://eceuropaeu.sharepoint.com/sites/eacea-budget-finance/SitePages/Access-to-Financial-Tools.aspx)