Ref. Ares(2026)6556349 - 30/06/2026

EUROPEAN HEALTH AND DIGITAL
EXECUTIVE AGENCY (HaDEA)

RECORD OF PERSONAL DATA PROCESSING ACTIVITY OF ePROCUREMENT PROCEDURES AND CONTRACTS MANAGMENT ON THE PORTAL (SEDIA)

*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)

Record No: - Fin 05 **Initial approval by Data Controller**: 30/06/2026

Update (s): n/a

IDENTIFICATION OF THE DATA CONTROLLER

European Health and Digital Executive Agency (HaDEA), Director and competent Heads of Department/ Heads of Unit, COV2, Place Charles Rogier 16, B-1049 Brussels, Belgium

GROUND FOR THIS RECORD

- □ Record of a new type of processing activity of personal data (before its implementation)
- **X New record of a processing activity of personal data that is already in place**
- □ Change/Amendment/ Update of an already existing previous record

DESCRIPTION OF THE PROCESSING ACTIVITY

This record relates to the processing of personal data via the EU Funding & Tenders Portal (and the EU Funding & Me mobile application, together the "Portal" or FTOP), the related Single Electronic Data Interchange Area (SEDIA)[2], ABAC and SUMMA[3], by EU institutions and bodies acting as

[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).

[2] SEDIA is the business and IT solution by which the handling of eProcurement related information is processed.

Joint Controllers for Procurement procedures and contracts of EU programmes and initiatives delegated to and managed by the Agency: EU4HEALTH Programme, SMP/Food Programme, parts of the Horizon Europe Framework Programme and other procurements.

The management of the procurement procedures and the resulting contracts in accordance with the EU Financial Regulation[4] and the Agency's Procedure on public procurement require the processing of personal data in compliance with the Regulation (EU) 2018/1725.

The record covers the entire life cycle of personal data processing activities for all electronic and paper based transactions, including registration, accreditation, application, selection, evaluation, validation, entry into and monitoring of relevant type of legal commitment, implementation of the contract and services and all linked financial transactions, including the use of specific IT tools.

European Institutions and bodies using FTOP/eGrants have signed a Joint controllership agreement. This record is based on the corresponding record of the European Commission DPR-EC-33848.1.

[3] The Commission DG BUDG manages ABAC - the financial and accounting applications set up by the Commission to monitor the execution of its budget and to prepare its accounts -, and SUMMA - the Commission's next-generation corporate financial system.

[4] Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council of 23 September 2024 on the financial rules applicable to the general budget of the Union (recast) (hereafter the “Financial Regulation”) and its predecessor, Regulation (EU, Euratom) 2018/1046.

1. INFORMATION ON THE PROCESSING ACTIVITY
of eProcurement procedures and contracts management on the Portal (SEDIA)

This processing activity is performed in accordance with **Regulation (EU) No 2018/1725**[5] 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.

The management of procurement procedures, the evaluation of tenders, the award and management of contracts by the EU institutions and bodies requires the processing of personal data in compliance with the Regulation.

1.1. The Data Controller is:
European Health and Digital Executive Agency (HaDEA) Director who delegates to the competent Head of Unit or Head of Department responsible for the procedure, COV2, Place Charles Rogier 16, B-1049 Brussels, BELGIUM can be contacted at:

HADEA-PROCUREMENT@ec.europa.eu

1.2 The contact details of the Data Portection Officer (DPO)

HADEA-DPO@ec.europa.eu

1.3 Joint controller:

Joint controllership is involved.

Linked to the EU Funding & Tenders Portal ("the Portal"), the European Commission's central online platform for accessing EU funding and procurement opportunities and SEDIA, a strategic initiative of the European Commission aiming at creating a master data repository of external stakeholders conducting business with the European Commission, specifically through grants or tenders.

All EU institutions and bodies using the EU Funding & Tenders Portal and the EU Funding & Me mobile application (together the "Portal" or FTOP) (SEDIA) act as Joint Controllers:
list-of-joint-controllers_en.pdf

The essence of the Joint Controllership Arrangement is available in the the corresponding record of the European Commission DPR-EC-33848.1.

The joint processing operations consist of the following processing activities:

- Definition of purposes and design of the related means (business processes and IT systems) for processing operations related to the management of procedures and contracts via the SEDIA corporate initiative;

- The entire life cycle of linked personal data processing operations, including (but not limited to) submission of requests to participate and tenders, evaluation (access to market, selection criteria,

[5] 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).

exclusion criteria and award criteria), entry into relevant type of legal commitment and all linked financial transactions.

The EC services (namely DG DIGIT, DG RTD and JRC) are the primary service providers, carry out parts of the processing operations for the Commission departments and to some extent to the Executive Agencies. As service providers, they may facilitate and manage the EU public funding related business processes for all potential participants to any EU funding programme executed via the SEDIA corporate initiative, which imply:
- The design of the related means (business processes and IT systems) for all processing operations related to the corporate management of contracts via the SEDIA corporate initiative;
- Secured access rights and controls via the European Commission Authentication Service (ECAS);
- Storage services for the collected/processed data in electronic format.

DG DIGIT implements and maintains the accounting IT tool ABAC and the new corporate financial system SUMMA.

1.4 The following entity(ies) is/are acting as Processor(s):

The independent expert assisting evaluation, reviewers and other external contractors (including in-house service providers and extra-muros). All of them are working on behalf of and under the responsibility of HaDEA for the purposes of managing procurement procedures and contracts (including checks and reviews).

For HaDEA and certain related services (e.g. TEAMS etc), EC/DG DIGIT may act as a processor with its contractor (Microsoft, Cisco) under the relevant contract.

1.5 Description and purpose(s) of this processing:

The purpose is to process operations relating to eProcurement procedures and contract management, which include (but are not limited to):

- Submission of requests to participate and tenders;

- Q&A, Helpdesk functions;

- Evaluation (access to market, selection criteria, exclusion criteria and award criteria, opening and evaluation of offers, etc);

- Entry into relevant type of legal commitment and all linked financial transactions;

- Contract management, including adaptation, preparation, and amendments; including advanced/intermediate/final payments, deliverables, and reporting;

- Contribution to the EC reporting on socio-economic data or any other aspects;

- Publication and dissemination of contract information and results and exploitation of results;

- Follow-up of publications generated by the contracts and possible related questions such as IPR, etc

- Communication;

- Contribution to the design, monitoring and evaluation of the EU funding programmes and policy development performed by the EC.

The record covers all processes related to contract management (including but not limited to signature, amendments, reporting, payments).

The record also covers all internal and external checks, audits, investigations and other proceedings, that users of public funds of European Union are subject to, to assess the legality and regularity of the transactions underlying the implementation of the European Union budget. The audit and control activities can be conducted at any time during the performance of the programme/contract, as well as thereafter, and can concern any aspect, depending on the needs of the contracting authorities. The

audit and control activities may be carried out on documents; and/or on the spot in any place where the funds in question are managed or used; the geographical scope is therefore worldwide.

The record covers both external and internal data subjects. The Joint Controllers may use limited personal data obtained through the Portal for the purposes of monitoring, evaluating, and improving their programmes and initiatives; to account for these in front of the legislative authorities (the European Parliament and Council of the European Union); to comply with their public reporting obligations; and as a source of information for policy-making.

The personal data will not be used for an automated decision-making, including profiling.

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[6] laid down in Union law[7]:
and 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[8];

(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

[6] 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

[7] Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council of 23 September 2024 on the financial rules applicable to the general budget of the Union (recast), in particular Titles V (Common Rules); VII (Procurement and Concessions);

Regulation (EU) 2021/522 establishing a programme for the EU's action in the field of health (EU4health programme) for the period 2021–2027;

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).

Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination

[8] Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council of 23 September 2024 on the financial rules applicable to the general budget of the Union (recast), in particular Titles V (Common Rules); VII (Procurement and Concessions);

The financing decisions form part of the legal basis for a processing operation, where applicable, in line with Article 110 of the Financial Regulation;

Regulation (EU)2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, in particular recital (87) and Article 53 and 54;

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;

Council Regulation (EC) No 58/2003 of 19 December 2002 laying down the statute for executive agencies to be entrusted with certain tasks in the management of Community programmes;

more specific purposes.

Reasons supporting the lawfulness of the data (explanation to why the processing is necessary)

The processing is necessary for HaDEA to carry out its budget implementation tasks, awarding and entering into contracts with a view to the acquisition of works, services, supplies or buildings by HaDEA (including for inter-institutional or joint procurement procedures).

Description/additional information regarding the lawfulness and fairness
The processing performed satisfies the principles of lawfulness and fairness: processing is necessary for the performance of tasks that the EU legislation forsees for HaDEA; processing is necessary to comply with specific legal obligations (in particular related to audits) to process personal data; processing is necessary for the performance of the contracts to which the data subjects are parties and for the preliminary steps for entering into such contracts; processing concerns personal data of individuals who have consented to it.

1.7 The categories of data subjects

Agency staff (Contractual and temporary staff in active position)

- Agency's staff involved in the procurement procedures and contracts management

Outside of to the Agency:

- Staff of the European Commission and of other Union institutions, bodies and agencies (EUIBA) involved in the procurement procedures and contracts management;
- External experts providing expertise to the procurement procedure;
- Natural persons who are: economic operators, tenderers, contractors (including in-house service providers, consultants, and extra-muros service providers), subcontractors, staff of contractors, subcontractors, and other entities on which a tenderer relies, members of the evaluation committees.
- Third-party platform provider authorised by the Commission/HaDEA.

1.8 Categories of personal data

a) Categories of personal data:

Identification data: first name, middle name & last name (including maiden name), gender, title, nationality, Participant Identification Code (PIC) (when the participant is a natural person), other person identifiers linked to other sources (e.g. ORCID ID or Researcher ID), ID document number (passport/other);

- Contact data: e-mail, contact (phone) numbers – including all types, such as personal, business, GSM, landline, fax, voice over IP etc., personal address(es) submitted (such as origin, permanent, current, previous residences);

- Employment and career related data: current employment status (such as employer's name & address, department, function/position, staff category), employment contracts, salaries, timesheets, missions/meetings minutes/reports, supporting documents related to travel costs, work experience and professional expertise;

- Financial data of natural persons: bank account related data (such as account number, name and address of the holder, name and address of the bank), ownership and tax related data (such as revenues and patrimony, number / value of shares or voting right held by natural persons or group of natural persons, social security contributions, VAT and other taxes paid);

- Data necessary for management of procedural /evaluation/performance related aspects: eligibility (access to procurement market) criteria related personal data, exclusion criteria related personal data (including declaration on honour and extracts from judicial records for natural persons), selection criteria related personal data, award criteria related personal data, performance related personal data linked to legal commitment with HaDEA (such as quality of performance of participant (if a natural person) or participant's staff during the execution of relevant legal commitment, any other procedural (application, evaluation process related, contract reporting and monitoring etc.) data that is of personal nature and linked to points listed above;

- Authentication and access data: EU Login credentials, IP address, security data/log in files;

- Other incidental and unsolicited data: third party personal data: the supporting documents submitted by the participant may contain personal data of third persons (such as other experts mentioned in proposals, 7 board members etc.) not necessary for purposes of processing, data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and sexual orientation - if these data appear in the documents (CVs, ID documents, other documents) provided by the data subjects without the request of REA, (references to) personal data freely available on social networks and the Internet, personal data that could be incidentally transmitted to HaDEA (although not solicited) in the context of the contractual obligation of the contractors to report on ethics and Code of conduct matters.

The data categories listed above are exhaustive, but the listed data fields are non-exhaustive.

b) Categories of personal data processing likely to present <u>specific risks:</u>

Official extract of judicial/police record may be requested by the responsible authorising officer (RAO) to prove the absence of exclusion of the entity or related persons.

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

Data subjects may provide voluntary health-related data for obtaining additional reimbursement due to special needs and possible additional costs. In addition, in the course of its audit/control activities, HaDEA might process special categories of personal data (related to maternity, illness, special leaves).

- Health related data: information related to health conditions in relation to claims (e.g. for special costs or triggering a change for a contractual condition (suspension, amendment, parental leave etc.);

The reasons under Article 10(2) allowing the processing of the special categories of data

Such processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the entity of the controller or of the data subject in the field of employment and social security.

Processing is necessary for reasons of substantial public interest, on the basis of Union law which shall be proportionate to the aim pursued.

_____

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

HaDEA applies the principles and retention periods indicated in Common Retention List of the Commission by analogy.

Personal data shall be stored for no longer than is necessary for the achievement of the purposes for which the data was collected or further processed.

- Data related to managing award procedures (for unsuccessful tenderers and candidates) – retention period of maximum 5 years after the end of the year of the call submission deadline.

- Data related to management of contracts (contractors, subcontractors, guarantors) – retention period of maximum 10 years following the final payment made under the contract.

- Any extracts from judicial records provided by the data subjects are not kept longer than 2 years after the end of the year in which the particular procedure was accomplished.

Data will be deleted at the end of this period.

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

The personal data may be further processed for historical, statistical or scientific purposes.
In such cases, these personal data are clearly identified, and appropriate safeguards are in place to ensure data minimisation: pseudonymisation.

At the end of the pre-defined retention period, the files are usually subjected to sampling for transfer to the Commission's historical archives for further conservation. The vast majority of files are not sampled and are destroyed. In the rare occurrence that a file is selected or sampled at the end of the retention period, some data may be retained in the Commission's Historical Archives. Any retention of data may be temporarily extended if a monitoring, audit on inspection task in application of European law (e.g. internal audits, the Panel referred to in Articles 93 and 145 of the Financial Regulation, European Anti-fraud Office - OLAF or Court proceedings) are ongoing; any action performed in corporate eProcurement IT systems by data subjects under their EU login is recorded in order to enable queries on financial, contractual and accounting matters as well as for audit trail purposes.
The further retention time for this purpose will be up to 25 years.

1.10 The recipient(s) of the data

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

Within the Agency:

Based on the need-to-know principle:

The Director of the Agency;

HaDEA Operational and/or Administrative Units in charge of the call for tenders, procurement, the management of the contract, financial and legal matters as specified in the relevant data protection notice;

In case of audits or proceedings, etc., HaDEA's Internal Controller, Data Protection Officer, Legal Affairs Sector, etc.

Outside the Agency:

Based on the need-to-know principle:

• Any EUIBA working with the Portal processing operations covered by the privacy statement or entitled by law, and any legal and natural persons who is covered by the privacy statement and is in a 9 contractual relationship with Union institutions, bodies and agencies (EUIBA).

• DG Budget (BUDG) for Legal Entity and Bank Account Files, ABAC and SUMMA;

• Secretariat-General (SG) – Ares;

• DG for Informatics of the European Commission (DIGIT) - Outlook, shared drives, IT systems;

• any natural/legal person with whom Union institutions, bodies and agencies are under regulatory duty; or who needs the data in the public interest, , if the recipient needs the data for legitimate performance of tasks within its competence (such as: authorized persons representing the Member States; EEA countries; and associated or beneficiary third countries (if relevant for the programme) in various programming/legislative bodies (programme committees; advisory groups; national authorities/agencies; contact points etc.); authorized persons representing the industry in the case of the EU joint-undertakings' operations etc.);

• any natural person who has a contractual relationship with a joint controller and who is working as processors on behalf of the Agency in various stages of the procurement procedures (publication, evaluation, contract execution, checks, reviews, ex-post controls), if applicable;

• any natural/legal person who has a contractual relationship with a joint-controller and who is working on behalf of and under the responsibility of that joint-controller for the purposes of performing the tasks of the relevant contract, or has a need-toknow stemming from the contract (external experts);

• authorised staff of contractors acting as processors for a specific processing operation (external auditors; event organisers), etc.

- 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.

  This transmission is restricted to the information necessary for the legitimate performance of tasks within the competence of the recipient. The recipients of the data are reminded of their obligation not to use the data received for other purposes than the one for which they were transmitted.

The public (any person)

In case an economic operator is awarded a contract by the Agency, personal data may be made public. Information may be disclosed to the public in accordance with the Commission's obligation to publish information on the outcome of the procurement procedure and on the beneficiaries of funds deriving from the budget of the European Union (Article 38 (2) of the Financial Regulation).

This information concerns in particular the name and address of the economic operators, amount awarded and the name of the project/programme (where applicable) for which contract is awarded. This information is published in supplement S of the Official Journal of the European Union on the website of the Commission (see the Financial Transparency System).

1.11 Transfers of personal data to third countries or international organisations

In general, personal data **will not be transferred to third countries** or **international organisations.**

Transfer may occur under certain procurement procedures and contracts in the context of evaluation of tenders and award of contracts to persons/entities from non-EU/EEA countries, when necessary for HaDEA to carry out its budget implementation tasks, or to comply with its obligations under the applicable legislation and specific agreements with the international organisations.

HaDEA may transfer personal data to recipients in a third country in accordance with the Regulation.

Personal data may be transferred to the following recipients in non-EU countries: non-EU based contractors;

Legal basis: Art 47 and 48; for specific situations derogations may apply: Art 50 of the Regulation.

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 a constant evolution.

Personal data in electronic format (emails, documents, databases, etc.) that are processed during this processing activity are stored on the servers of the European Commission. All Commission IT systems are compliant with the Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission.

In addition, external contractors run IT systems on behalf of the Commission in line with the provisions of Regulation 2018/1725. They act only upon written instructions from the Controllers and undertake to adopt appropriate technical and organisational security measures having regard to the risks inherent to the processing and to the nature of the personal data concerned. Appropriate technical and organisational security measures are in place to address all data processing risks (preventing unauthorised access, reading, copying, alteration or deletion of personal data etc.).

Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into consideration the risk presented by the processing and the nature of the personal data being processed. Organisational measures include restricting access to personal data solely to authorised persons with a legitimate need-to-know for the purposes of this processing operation. Access to data is only available to registered users as approved by their hierarchy through a separate access control module (EU Login and SECUNDA+), and according to the need-to-know principle. The security module logs which user has requested access to the system, together with the date and timestamp. Authentication is based on the EU Login mechanism.

The access rights for the accounting system are defined via the accounting system security modules. The authentication to the accounting system, the document management system etc. is accomplished via the EU Login mechanism, which is designed to increase the security of Commission's IT systems.

The paper files are stored in locked/secured cupboards and /or storage offices. Access is limited and is on a need-to-know basis.

1.14 Data protection Notice and information on Data subject rights/restrictions

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.

Data Subjects are informed on the processing of their personal data via Privacy Statement available under the Legal notices page in the Portal, under this link:

EU Funding & Tenders Portal