PRIVACY STATEMENT

for the Expert Management PADR

1. INTRODUCTION
This Privacy Statement describes the measures taken to protect your personal data with regard to the action involving the present data processing operation and what rights you have as a data subject. EDA protects the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of personal data (Article 1.1 of Regulation No 2018/1725).
2. CONTROLLER OF THE PROCESSING OPERATION
EUROPEAN DEFENCE AGENCY Rue des Drapiers 17-23 B-1050 Brussels www.eda.europa.eu and European Commission
3. PURPOSE OF THE PROCESSING
The purpose of the processing operations is the registration, selection and management of external experts on the Participant Portal in the context of the Preparatory Action of Defense Research (PADR). If an expert is selected, he/she gets a contract for activities that involves the evaluation of proposals submitted under annual calls for proposals, monitoring of the implementation of actions, ethics reviews, checks and audit. Moreover, EDA will manage the reimbursement of expenses (travel expenses, etc.) the payment of allowances and fees, where applicable, and the subsequent management of the Experts and their contracts. The processing operation is necessary in order to proceed with the evaluation of project proposals requesting financial support from PADR, to participate as observers in the evaluation and/or to ensure monitoring of the implementation of actions, ethics reviews, checks and audit. External experts may also be contacted by the Controller or their contractors for voluntary surveys.
4. DATA PROCESSED
Data processed are the following:

The personal data collected and further processed via the Expert Area of the Participant Portal are identification data, contact data, and professional data:

- Identification data: title, first name, family name (current and former), gender, date of birth, nationality & candidature reference;

-Contact details: phone(s), fax and email address, physical address (street, town, post code, country);

-Education: language level, titles of qualifications, subject or field, name of institution, country, and year awarded;

-Area of expertise: specialization, research interest, related keywords;

-Career: Host Institution/organization, current and previous employments (organization name, department sector, job title, employment dates, town or city, country, organization type and size), total number of years of experience related to the field of expertise required, current employment status, experience in the industrial sector (if applicable), information concerning assistance to the European Commission in its research programmes (area of work and dates are mentioned in a free text field). Description of other experience in evaluation, peer review, monitoring, programming, including the name of the organization, year and role, being in possession of a security clearance;

-Publications: title, date of the publication, authorship, name of publisher/journal, keywords. The data can be entered manually or be retrieved via a Digital Object Identifier (DOI) entered into the system.

-Achievements: date, country and nature of achievement, reference for patents;

-Other categories of data: Funding programme for which the expert wishes to be considered, free field where the expert can provide additional information or links of interest (e.g. to CV).

-Researcher ID1 (optional).

The controllers do not need to collect, and process special categories of data as defined in Article 10 of Regulation 2018/1725 except in the following specific circumstances:

a) It is needed to acquire extracts of judicial records for the detection of fraud related to the contract or procedures relating to sanctions according to the Financial Regulation and its Rules of Application.

b) The data subjects are free to provide voluntary health-related data due to their special needs in order to be refunded of possible additional costs relating to the subsequent accommodation and travel specificities. Any controllers' staff member in charge of the processing of health-related data would be subject to the specific obligation of secrecy equivalent to that of a health professional and might be requested to sign a specific professional secrecy declaration and might be requested to sign a specific professional secrecy declaration, if necessary.

Irrelevant or excessive data are not retained by the Controllers.

5. RECIPIENTS OF THE DATA

The category of recipients are:

- EU institutions and bodies;
- Member States;

- Third parties in the European Economic Area (EEA) and in countries for which the Commission has adopted and adequacy decision;
- The public.

For more details, please refer to the "List of recipients", published in the Privacy Statement of the Participant Portal. Disclosure to some categories of recipients require the prior consent of the data subject.

6. PROTECTION AND SAFEGUARDING OF THE DATA

All data in electronic format (emails, documents, uploaded batches of data, etc.) are stored either on the servers of the European Commission or of its contractors, the operation of which abide by the European Commission's security decision of 16 August 2006 (C(2006)3602) concerning the security of information system used by the European Commission.

Access rights and controls are secured via the European Commission Authentication Service (ECAS) granted to persons authorized to get access to specific documents (call management, grant management, etc.)

All stakeholders involved in the evaluation and granting process are reminded to use the personal data received only for the purpose for which they were transmitted and to disregard all irrelevant and excessive data received with the proposals.

The personal data is stored in databases and servers that reside on the Controller's premises, the operations of which abide by Council's security regulations as set out in the Council Decision 2013/488/EU.

Finally, contractors are bound by a specific contractual clause for any processing operations of personal data on behalf of the Commission and EDA, and by the confidentiality obligations.

7. RIGHT OF ACCESS AND RECTIFICATION OF THE DATA

At any time, data subjects can access/verify/modify/ their personal data online upon logging on to the Expert area in the Parliament Portal. They may also change their European Commission Authentication Service (ECAS) password which allows them to login to the system and update their personal information contained in their profile. The data subjects can also change at any time their choice for the opt-ins regarding access to their personal data.

In case they wish to delete their personal data, data subjects should send an email to the European Commission (Controller) using the following functional mailbox: ec-expert-area@ec.europa.eu

For local repositories, they can contact the Controller under PreparatoryAction@eda.europa.eu.

Data subjects have the right to have recourse to the European Data Protection Supervisor (EDPS@edps.europa.eu) preferably after a first contact with their Controller(s).

With regard to erasure/blocking, further to justified legitimate request of the data subject:

-Time limit to rule on a request: 15 working days (beginning from the reception of the request);
-Blocking period: On a case-by-case basis, but immediately if applicable (maximum delay of 5 working days);
-Ensure Period: Maximum delay of 5 working days after the ruling on the request (if applicable).

8. TIME LIMIT FOR STORING DATA

- For experts not yet selected by a Controller, their personal data are kept for the duration of the related programme's activities for which they have registered.

- For experts selected by EDA, personal data are kept for 5 years after the end of the particular programme on which they provided their services.

Should the need arise to acquire extracts of judicial records for the detection of fraud related to the contract or procedure relating to sanctions according to the Financial Regulation and its rules of application, those extracts shall not be kept longer than two years after the accomplishment of the particular procedure.

Supporting documents relating to budget implementation are kept for at least five years from the date on which the European Parliament grants discharge for the budgetary year to which the documents relate. The personal data contained in this type of supporting documents shall be deleted where possible when those data are not necessary for budgetary discharge, control and audit purposes.

Personal data contained in supporting documents are deleted where possible when these data are no longer necessary for budgetary discharge control and audit purposes.

Experts are asked to indicate if they wish that their data be retained in the database of experts beyond this date in order to be considered for assignments for the forthcoming programme. If they do not wish to be considered for future assignments, their data are deleted after the end of the programme.

-For unsuccessful and withdrawn experts, personal data may be retained only for up to 5 years after the end of the particular procedure to allow for all possible appeals.

Anonymous or encrypted data can be retained for a longer period for statistical, historical or scientific purposes.

Statistics on experts' nationality, gender, field of expertise for example may be generated during the implementation of the programmes and also after their end, in a form that safeguards the data subject's anonymity.

In addition, as referred to above, statistics on experts with contracts (name, first name, candidature number, number of days worked) may be generated during the implementation of the programmes, to comply with the rules on rotation of the experts.

These statistics will be retained for the duration of the PADR.

9. LEGAL BASIS FOR THE PROCESSING OPERATION

Articles 5(a), 5(c) and/or 5(d);
Article 31 of Council Decision (CFSP) 2015/1835 of 12 October 2015 defining the statute, seat and operational rules of the European Defence Agency.

10. CONTACT DPO

In case you have any questions or queries concerning data protection at the European Defence Agency, you can also contact the Data Protection Officer at dataprotection@eda.europa.eu.

11. RECOURSE TO EDPS

As a data subject you have the right to have recourse at any time to the European Data Protection Supervisor (http://www.edps.europa.eu) at edps@edps.europa.eu.

12. ADDITIONAL INFORMATION

More information on Data Protection at the European Defence Agency can be obtained on our public website https://www.eda.europa.eu/Aboutus/how-we-work/data-protection.