



EUROPEAN COMMISSION

PROTECTION OF YOUR PERSONAL DATA

This privacy statement provides information about the processing and the protection of your personal data.

Processing operation: FPI contribution agreements with entities implementing EU funds under indirect management in the area of Common Foreign and Security Policy (CFSP) / Common Security and Defence Policy (CSDP)

Data Controller: Service for Foreign Policy Instruments, Unit FPI.3

Record reference: DPR-EC-04626

Table of Contents

- 1. Introduction**
- 2. Why and how do we process your personal data?**
- 3. On what legal ground(s) do we process your personal data?**
- 4. Which personal data do we collect and further process?**
- 5. How long do we keep your personal data?**
- 6. How do we protect and safeguard your personal data?**
- 7. Who has access to your personal data and to whom is it disclosed?**
- 8. What are your rights and how can you exercise them?**
- 9. Contact information**
- 10. Where to find more detailed information?**

1. Introduction

The European Commission (hereafter ‘the Commission’) is committed to protect your personal data and to respect your privacy.

The Commission collects and further processes personal data pursuant to 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 (repealing Regulation (EC) No 45/2001).

This privacy statement explains the reason for the processing of your personal data, the way we collect, handle and ensure protection of all personal data provided, how that information is used and what rights you have in relation to your personal data. It also specifies the contact details of the responsible Data Controller with whom you may exercise your rights, the Data Protection Officer and the European Data Protection Supervisor.

The information in relation to the processing operation “*FPI contribution agreements with entities implementing EU funds under indirect management in the area of Common Foreign and Security Policy (CFSP) / Common Security and Defence Policy (CSDP)*”, undertaken by the Service for Foreign Policy Instruments (FPI), Unit FPI.3, is presented below.

Please note that a separate privacy statement concerns FPI contribution agreements with entities implementing EU funds under indirect management, excluding CFSP.

2. Why and how do we process your personal data?

Purpose of the processing operation:

The controller collects and uses your personal data for the negotiation, conclusion and implementation of contribution agreements concluded between the Commission and entities implementing EU funds in indirect management in the area of Common Foreign and Security Policy (CFSP) / Common Security and Defence Policy (CSDP) under Article 62(1) (c) (viii) of Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union (OJ L 193, 30.7.2018, p.1, the Financial Regulation).

Data processing operations concern the following purposes in the area of CFSP operations:

- the management, coordination and organisation of ex-ante assessment procedures in the context of the pillar assessment exercise and in the context of ex-ante verifications. Ex-ante verifications concern only non-pillar assessed entities. Once an entity is pillar-assessed, FPI no longer makes ex ante verifications;
- the management, coordination and organisation of the procedure leading to the preparations and conclusions of the corresponding contribution agreements, their possible amendment/s and their closure;
- the management, coordination and organisation of the implementation of the contribution agreements;
- generally, the implementation of EU funded external actions stipulated in these contribution agreements by the partner entities (Cf. CSDP Missions, EU Special Representatives, Article 28 TEU Actions implementing entities, Warehouse operator and implementing entities of Non-Proliferation and Disarmament projects).

Your personal data will *not* be used for an automated decision-making including profiling.

3. On what legal ground(s) do we process your personal data

We process your personal data, because 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 [Article 5(1)(a) of Regulation (EU) 2018/1725].

Within the European Commission, the mission of the Service for Foreign Policy Instruments (FPI) is to support the attainment of the objectives of the EU foreign and security policy as defined in Article 21 of the Treaty on European Union, in particular as regards peace and conflict prevention.

For that purpose FPI is responsible, under the authority of the High Representative of the Union for Foreign Affairs and Security Policy in his/her capacity as Vice-President of the Commission, for the operational and financial management of the EU budget for Common Foreign and Security Policy (CFSP).

According to Article 62(1)(c)(viii) of the Financial Regulation¹, budget implementation tasks in the indirect management mode may be entrusted to bodies or persons entrusted with the implementation of specific actions in the CFSP pursuant to Title V of the TEU. These bodies or persons are identified in the relevant basic acts under CFSP (Cf. all the relevant Council Decisions).

Based on this, the Commission adopts a financing decision (a Commission Decision implementing the Council Decision), which is then operationalised through the conclusion of an agreement (namely, a contribution agreement) with a partner entity that is thereby entrusted with the management of funds.

The contribution agreement details the action (i.e. its objectives, expected outputs and indicative activities), the tasks to be implemented by the entity, as well as the respective rights and obligations of the Commission, as contracting authority. The contribution agreement also stipulates the tasks and responsibilities of the partner entity, as the Commission partner entrusted with the implementation of funds, pursuant to Articles 154 to 158 of the Financial Regulation.

4. Which personal data do we collect and further process?

In order to carry out this processing operation, FPI.3 Unit collects the following categories of personal data:

A. Personal data of members of the staff of FPI in the HQ, which may include in particular: name; function; title; business contact details (e-mail address, business telephone number, mobile telephone number, fax number, postal address, department and office number, country of residence); signature; opinions.

¹ Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012 (OJ L 193, 30.7.2018, p.1);

B. Personal data of representatives/staff of the entities concluding agreements with the Commission and/or acting as contact points, which may include in particular: name; function; title; business contact details (e-mail address, business telephone number, mobile telephone number, fax number, postal address, department and office number, country of residence); signature; opinions.

C. Personal data of Heads of Missions and EU Special Representatives who are employed by the Commission as Special Advisors, which may include in particular: name; function; title; CVs; documents and own declarations clarifying the family situation for the purposes of the determination of allowances (certificates of school attendance by children, income of spouses etc.)

D. Personal data of successful candidates for employment in non-pillar assessed CSDP Missions and EU Special Representatives, which may include in particular: name; function; title; CVs; application forms with information on the professional career and studies; documents proving the professional experience (letters and certificates from previous employers, previous employment contracts); documents proving the completion of university or secondary studies.

E. Personal data of tenderers of non-pillar assessed CSDP Missions and EU Special Representatives, which may include in particular: name; function; title; business contact details (e-mail address, business telephone number, mobile telephone number, fax number, postal address, company and department, country of residence, internet address).

F. Personal data of tenderers, grant applicants, contractors, subcontractors found by the partner entity and/or the Commission to be in an exclusion situation, which may include in particular: name; function; title; business contact details (e-mail address, business telephone number, mobile telephone number, fax number, postal address, company and department, country of residence, internet address); final judgments/decisions declaring the person to be in one of the exclusion situations set out in Article 136 of the Financial Regulation.

We have obtained your personal data from

- the entity submitting the application for ex ante assessment;
- the entity you are representing/are working for.

5. How long do we keep your personal data?

FPI.3 Unit only keeps your personal data for the time necessary to fulfil the purpose of collection or further processing. The retention periods are aligned with the Common Commission-Level Retention List (CRL)² of the European Commission.

The personal data in connection with the CFSP activities under the referred contribution agreements under indirect management will be kept for 10 years.

6. How do we protect and safeguard your personal data?

All personal data in electronic format (e-mails, documents, databases, uploaded batches of data, etc.) are stored on the servers of the European Commission. All processing operations are carried out pursuant to the [Commission Decision \(EU, Euratom\) 2017/46](#) of 10 January 2017 on the security of communication and information systems in the European Commission.

² Annex 1 to SEC(2019)900.

In order to protect your personal data, the Commission has put in place a number of technical and organisational measures in place.

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. All the relevant files are stored in a locked archive room, specifically used only for CFSP activities.

Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purposes of this processing operation.

7. Who has access to your personal data and to whom is it disclosed?

Access to your personal data is provided to the Commission staff responsible for carrying out this processing operation and to authorised staff according strictly to the “need-to-know” principle. Such staff members abide by statutory, and when required, additional confidentiality agreements.

Recipients within the EU organisation:

- Staff of operational and financial units of FPI in the HQs participating in management of ex-ante verifications, in negotiation, conclusion and implementation of agreements with partner entities and in monitoring of implementation of specific actions by the partner entity – contracting authority under indirect management.
- Staff of OLAF, IDOC, IAS (Internal Audit Services), European Court of Auditors and the Legal Service of the Commission as well as staff of other DGs (SG, DG BUDG) upon request necessary in the context of official investigations or for audit purposes.
- The European Parliament and the Council upon their request, in accordance with Article 155(7) of the Financial Regulation.

Recipients outside the EU organisation:

- Partner entity representatives/staff, solely for the purpose of performance, management and monitoring of ex – ante assessments, of management and monitoring of contribution agreements concluded between the Commission and the partner entity and for enabling the Commission to comply with its obligations under the applicable legislation and under the abovementioned agreements with the entity.

Transfer of personal data to third countries:

Transfers of personal data outside of the EU or the EEA are likely to occur in the context of conclusion and implementation of agreements between the EU and the partner entities, for the Commission to carry out its tasks and to comply with its obligations under the applicable legislation and the agreements with the partner entities.

In particular, the Commission might transfer personal data to partner entities, namely CSDP Missions, EU Special Representatives, entities entrusted with the implementation of Non Proliferation and Disarmament projects, entities entrusted with the implementation of Article 28 Treaty of European Union Actions and International Organisations with which the Commission has signed a contribution agreement pursuant to Article 155(6) of the Financial Regulation. Such transfers are very limited and strictly necessary to enable communication between the parties to the agreements and to allow the Commission to comply with its obligations under the applicable legislative framework and to the agreements with partner entities. Transfers of personal data to

the partner entities take place on the basis of derogations set out in Article 50(1) (d) of Regulation (EU) 2018/1725 as they are necessary for reasons of important public interest.

On the other hand, in indirect management, the partner entity contracting authority makes available personal data it collected to the Commission to allow the Commission to exercise its supervisory powers.

At the level of agreements with partner entities, the Commission does not make available personal data, other than:

A. Personal data of members of the staff of FPI and/or any service provider of FPI involved in procedures of ex-ante assessments, negotiation/conclusion/implementation of agreements with partner entities. The types of personal data may include in particular: Name; Function; Title; Business contact details (e-mail address, business telephone number, mobile telephone number, fax number, postal address, department and office number, country of residence); Signature;

B. Personal data of persons and/or entities found to be in an exclusion situation, made available by the Commission to the partner entity, may include in particular: Name; Function; Title; Business contact details (e-mail address, business telephone number, mobile telephone number, fax number, postal address, department and office number, country of residence); Final judgments/decisions declaring the person to be in one of the exclusion situations set out in Article 136 of the Financial Regulation. These transfers are processed through the Commission's EDES system – see notification [DPO-3853 DG BUDG Entry of a Data Subject in the Early Detection and Exclusion System \(EDES-DB\)](#).

The recipients of personal data in the partner entity and the instances in which personal data might be transferred include in particular representatives and/or staff of the partner entity acting as the interlocutors of the Commission staff. Personal data of Commission staff made available to the representatives/staff of the partner entity are very limited and strictly necessary for enabling communication. Information on persons and/or entities found to be in exclusion situations are made available to comply with the Commission's obligation under Article 142(5) of the Financial Regulation.

Partner entities are bound by contractual clauses on the protection of personal data and by an obligation of confidentiality contained in the respective agreements signed between them and the EU.

Please note that pursuant to Article 3(13) of the Regulation, public authorities (e.g. Court of Auditors, EU Court of Justice) which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients. The processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

The information we collect will not be given to any third party, except to the extent and for the purpose we may be required to do so by law.

8. What are your rights and how can you exercise them?

You have specific rights as a 'data subject' under Chapter III (Articles 14-25) of Regulation (EU) 2018/1725, in particular the right to access your personal data and to rectify them in case your personal data are inaccurate or incomplete. Where applicable, you have the right to erase your personal data, to restrict the processing of your personal data, to object to the processing, and the right to data portability.

You have the right to object to the processing of your personal data, which is lawfully carried out pursuant to Article 5(1)(a) on grounds relating to your particular situation.

You can exercise your rights by contacting the Data Controller, or in case of conflict the Data Protection Officer. If necessary, you can also address the European Data Protection Supervisor. Their contact information is given under Heading 9 below.

Where you wish to exercise your rights in the context of one or several specific processing operations, please provide their description (i.e. their Record reference(s) as specified under Heading 10 below) in your request.

In certain circumstances, data subjects' rights may be restricted pursuant to Commission Decision (EU) 2018/1962 of 11 December 2018 laying down internal rules concerning the processing of personal data by the European Anti-Fraud Office (OLAF) in relation to the provision of information to data subjects and the restriction of certain of their rights in accordance with Article 25 of Regulation (EU) 2018/1725. Where Commission services process personal data in instances referred to in Article 1(3) of the Commission Decision (EU) 2018/1962, they may, where necessary, apply restrictions in accordance with this decision. To that end, they shall consult OLAF, unless it is clear to the Commission service or executive agency concerned that the application of a restriction is justified under this decision.

9. Contact information

- The Data Controller

If you would like to exercise your rights under Regulation (EU) 2018/1725, or if you have comments, questions or concerns, or if you would like to submit a complaint regarding the collection and use of your personal data, please feel free to contact the Data Controller, Service for Foreign Policy Instruments, Unit FPI.3, FPI-DATA-PROTECTION@ec.europa.eu.

- The Data Protection Officer (DPO) of the Commission

You may contact the Data Protection Officer (DATA-PROTECTION-OFFICER@ec.europa.eu) with regard to issues related to the processing of your personal data under Regulation (EU) 2018/1725.

- The European Data Protection Supervisor (EDPS)

You have the right to have recourse (i.e. you can lodge a complaint) to the European Data Protection Supervisor (edps@edps.europa.eu) if you consider that your rights under Regulation (EU) 2018/1725 have been infringed as a result of the processing of your personal data by the Data Controller.

10. Where to find more detailed information?

The Commission Data Protection Officer (DPO) publishes the register of all processing operations on personal data by the Commission, which have been documented and notified to him. You may access the register via the following link: <http://ec.europa.eu/dpo-register>.

This specific processing operation has been included in the DPO's public register with the following Record reference: **DPR-EC-04626**