EUROPEAN COMMISSION

PROTECTION OF YOUR PERSONAL DATA

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

Processing operation: Personal data related to Logistic and Financial support of the CSDP Warehouse II processed through the IT Platform "Enterprise Resource Planning" (ERP)

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

Record reference: DPR-EC-03426.1

Table of Contents

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 (DPO) and the European Data Protection Supervisor (EDPS).

The information in relation to the processing operation "Logistic and Financial Support of the CSDP Warehouse II processed through the IT Platform "Enterprise Resource Planning (ERP System)", undertaken by the Service for Foreign Policy Instruments (FPI), Unit FPI.3, is presented below.

The Commission - Unit FPI.3, the European External Action Service (EEAS) - Civilian Planning and Conduct Capability Directorate (CPCC) and civilian CSDP Missions act as joint controllers as they determine together the purposes and means of processing personal data in the context of ERP. This privacy statement includes information about the collection and use of personal data solely by the Commission. Separate privacy statements will be communicated by the other joint controllers.

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

Purpose of the processing operation: FPI.3 Unit collects and uses your personal information recorded in the ERP to uphold a central database (ERP) or inventory and asset management for civilian CSDP Missions (the Missions) creating links between assets and Missions' personnel.

The ERP system is an innovative solution in the form of a database that provides the civilian CSDP Missions, the EEAS/CPCC and the Commission/FPI with a common system to manage the inventory and the assets of the Missions, as well as to perform other subsidiary functions regarding payrolls and salaries.

Under the ERP System, while FPI is responsible for the ERP financial module and the ERP procurement module related to the inventory and assets of the Missions, the EEAS is responsible for the ERP human resources module related to the inventory and assets of the Mission. This privacy statement covers the ERP finance and procurement modules.

The ERP System, in particular:

- facilitates the administration of the inventory and asset management of the Missions,
- increases the transparency of who has what in terms of assets and other valuable terms,
- simplifies the financial management of the CSDP Missions,
- facilitates the procurement process of assets,
- simplifies the planning and establishment of new CSDP Missions;
- facilitates the Missions, the CPCC, the FPI and the Member States (MS) with statistics and reports on inventory and asset management,

- supports the technical solution to broaden the scope of the ERP-system at a later stage in order to get a complete system for the management of the inventory and i. e. procurement.

The Finance Module of the ERP, in particular:

- facilitates the verification and the monitoring of the management of the operational budget of the CSDP Missions,
- facilitates the Missions, the CPCC, the FPI and the Member States (MS) with statistics and reports on salaries and payrolls, and
- facilitates the payment process on the basis of the data collected in ERP.

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],

- processing is necessary for compliance with a legal obligation to which the controller is subject[Article 5(1)(b) of Regulation (EU) 2018/1725].

Under Council Decision (CFSP) 2018/653 of 26 April 2018, the EU established a warehouse capability for civilian crisis management missions (Ref. OJ L 108/22 of 27.4.2018). The warehouse contributes to ensure rapid deployment key equipment and assets and the provision of appropriate support services for the civilian crisis-management operations. It ensures quick and continuous access by those missions to such equipment and assets.

The warehouse capability may also provide, as required, the same support with regard to equipment, assets and services, for other operational action of the Union under Article 28 of the Treaty on European Union and EU Special Representatives.

The Annex to said Council Decision include a list of key equipment and assets to be provided by the warehouse capability operator. The strategic stock comprises the key equipment and assets needed to deploy a civilian CSDP mission of up to 200 staff to any area of operation within 30 days. The key equipment and assets include the Enterprise Resource Planning (ERP) IT system.

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

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

- Identification data: Name, function, staff number, contact and location details (e-mail address, telephone number, mobile telephone number, fax number, postal address, company and department, country of residence, IP address), passport number, ID number.

- Financial data: bank account reference (IBAN and BIC codes), VAT number, income, allowance, and expenses, etc.

We collect this data because you provided it to us. The provision of personal data is mandatory to meet the Mission statutory requirements as well as employment contractual requirements. The Mission needs this data from its employees based on the employment relationship established with them.

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.

- Personal data such as enlisted above under point 4 are retained for 5 years after the end of service of the respective Mission Member for the purpose of audit and eventual investigation.

- In case of a judiciary procedure related to employment of contracted staff or tour of duty of the seconded staff, personal data is kept for 5 years after the final judgment was rendered.

- In case of a complaint launched before the European Ombudsman or before the European Data Protection Supervisor or an investigation conducted by OLAF or by EPPO or a verification by the European Court of Auditors, personal data is kept for 5 years after the closure of the case.

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.

The Commission's contractors are bound by a specific contractual clause for any processing operations of your data on behalf of the Commission, and by the confidentiality obligations deriving from the General Data Protection Regulation ('GDPR' Regulation (EU) 2016/679).

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. 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.

The warehouse operator is presently delegated to the Swedish Civil Contingencies Agency (MSB), which acts as data processor. MSB has introduced the following additional and aappropriate organisational and technical security measures:

- In its electronic format, the data will be stored on the MSB server located in Sweden. The collected personal data are processed by assigned staff members. Files have authorised access. The database is accessible only to the recipients with the authorised administrative or viewer rights with a legitimate need to know for the purposes of this processing operation.

- Measures are provided by MSB/FPI to prevent non-responsible entities from access, alteration, deletion, disclosure of data.

- 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.

- Security is also ensured by the safety measures built in the various IT applications used.

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 to the "need to know" principle. Such staff abide by statutory, and when required, additional confidentiality agreements.

Recipients of your data are the following:

- EEAS staff members, responsible for Logistics, IT, Finance and Procurement on a need to know basis
- Assigned CSDP Mission Members responsible for Logistics, Finance and Procurement – on a need-to-know/need-to-do basis
- Assigned staff of the MSB, in its capacity as data processor only on a need-to-know basis with only viewer rights. The MSB does not collect, alter or delete personal data. Secure storage of personal data will be ensured by MSB.

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.

The single contact point for handling your requests is the respective CSDP Mission, represented by the Head of Mission.

However, you have the right to exercise your rights towards each of the joint Data Controllers. You can exercise your rights by contacting FPI, 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.

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-03426.1.**