EEAS PRIVACY STATEMENT - DATA PROTECTION NOTICE

FOR THE PURPOSE OF

PROCESSING PERSONAL DATA RELATED TO PURCHASE REQUISITIONS AND PAYMENTS IN THE PURCHASE-TO-PAY (P2P) SYSTEM BY THE EEAS

1. INTRODUCTION

The protection of your personal data and privacy is of great importance to the European External Action Service (EEAS), including the Delegations of the European Union. You have the right under EU law to be informed when your personal data is processed [e.g. collected, used, stored] as well as about the purpose and details of that processing.

When handling personal data, we respect the principles of the Charter of Fundamental Rights of the European Union, and in particular Article 8 on data protection. Your personal data are processed in accordance with Regulation (EU) 2018/1725 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, aligned with Regulation (EU) 2016/679, the General Data Protection Regulation. In this privacy statement you find information about how the EEAS and EU Delegations process your personal data and what rights you have as a data subject.

2. PURPOSE OF DATA PROCESSING: Why do we process your data?

The purpose of the present processing activity is to automate the handling and processing of purchase requisitions, including operational initiation and verification and thus to increase efficiency and reduce potential errors and to avoid double/triple entries. The system increases the ability to track invoices and automatically send notifications to the system, ensuring that payment is always made on time and allows the finance department to track in real time what is ordered, received, invoiced and awaited. The system is integrated with ABAC.

3. DATA PROCESSED: What data do we process?

The data, including personal data, which may be processed for that purpose are the following:

Suppliers, contact persons, signatories of contracts:

- Name
- Contact data (like address, phone number, e-mail)
- Contract, delivery and invoicing data (like bank account or deliveries)
- Data on the Legal Entity Forms and Bank Account Files

Providers of timesheets:

- Name
- Times worked

Users:

- Name
- Login data (ID, login times)
- Activity data (approvals, rejections)

Other persons appearing on the scanned documents:

Data on the documents like name, position, contact data, signature are only on the documents and not processed further.

4. DATA CONTROLLER: Who is entrusted with processing your data?

The data controller determining the purpose and the means of the processing activity is the European External Action Service (EEAS). The EEAS Division entrusted with managing the personal data processing under the supervision of the Head of Division is the following organisational entity:

Support to Delegations Division, RM.BHR.6

5. RECIPIENTS OF THE PERSONAL DATA: Who has access to your data?

The recipients of your data may be

- Assigned staff of the EEAS in charge of managing contracts, of ordering, approving deliveries and of payments;
- Assigned staff of the EEAS in charge of internal audit controls and legal matters;
- Assigned staff of the SAAS contractor, Exact Software Belgium BVBA;
- Assigned staff from the Institutions or bodies charged with a monitoring, audit or inspection task in conformity with the European Union law. e.g.: staff of European Anti-fraud Office (OLAF), European Public Prosecutor's Office (EPPO), Investigatory and Disciplinary Office (IDOC), Internal Audit Services (IAS), European Court of Auditors (ECA), the Legal Service of the European Commission (also hereinafter Commission)as well as staff of other General Directorates(DGs) of the European Commission (Secretariat General, DG Budget and clearinghouse) and of other EU institutions upon request necessary in the context of official investigations or for audit purposes (e.g. internal audits, Financial Irregularities Panel referred to in Article 93 of the Financial Regulation, Exclusion Panel referred to in Article 143 of the Financial Regulation, OLAF);

- Assigned staff of the European Commission Directorate General for Budget (DG BUDG) with regard to the Legal Entity Form (LEF) and Bank Account File (BAF).

Personal data is not intended to be transferred to a third country or an international organisation, except where necessary for providing access to recipients as described above. In case of international transfers appropriate safeguards are ensured in accordance with Chapter V of Regulation (EU) 2018/1725. The given information will not be communicated to third parties, except where necessary for the purposes outlined above.

6. ACCESS, RECTIFICATION AND ERASURE OF DATA: What rights do you have?

You have the right of access to your personal data and the right to correct your inaccurate, or incomplete personal data taking into account the purpose of the processing. The right of rectification can only apply to factual data processed. Under certain conditions, you have the right to ask the deletion of your personal data or restrict their use as well as to object at any time to the processing of your personal data on grounds relating to your particular situation. We will consider your request, take a decision and communicate it to you without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary. For more detailed legal references, you can find information in Articles 14 to 21, 23 and 24 of Regulation (EU) 2018/1725. In specific cases, restrictions under Article 25 of the Regulation may apply. If you wish to exercise your rights or have questions concerning the processing of your personal data, you may address them to the Data Controller via the functional mailbox:

support-to-delegations@eeas.europa.eu

7. LEGAL BASIS: On what grounds we collect your data?

Data processing is lawful under article 5(1)a, Article 5(1)b and Article 5(1)c of Regulation (EU) 2018/1725: necessary for the management and functioning of the EEAS and to comply with the rules of sound financial management below as well as to execute the contract between the EEAS and the supplier.

Legal reference:

- Regulation (EU, EURATOM) No 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, "Financial Regulation", in particular Title V – Common rules, Title VII – Procurement and concessions and Annex I – Procurement

Further legal reference:

- Council Decision of 26 July 2010 establishing the organisation and functioning of the EEAS (2010/427/EU) – OJ L 201, 3/8/2010, p. 30.

8. TIME LIMIT FOR DATA STORED & SECURITY MEASURES: For what period and how we process your data?

Data are kept according to the legal rules governing procurement:

- Files relating to tender procedures, including personal data, are to be retained in the service in charge of the procedure until it is finalised, and in the archives for a period of 10 years following the closure of the contract in conformity with the Common Commission-Level Retention List (SEC(2019)900 second revision) as part of the e-Domec policy. However, requests to participate and tenders from unsuccessful tenderers have to be kept only for 5 years following the closure of the contract.
- Files related to implementation of contracts are kept by the EEAS or EU Delegation and by the data processor (contractor) for up to 10 years from the date on which the European Parliament grants discharge for the budgetary year to which the data relates (end of the contract).
- Files could be retained until the end of a possible audit if one started before the end of the above periods.
- After the periods mentioned above have elapsed, the files containing personal data are sampled and sent to the historical archives of the EEAS for further conservation, as applicable. The non-sampled files are destroyed.

Security of data: Appropriate organisational and technical measures are ensured according to Article 33 of Reg. (EU) 2018/1725. The collected personal data are stored on servers that abide by pertinent security rules. Data is processed by assigned staff members. Access to specific files requires authorisation. Measures are provided to prevent unauthorised entities from access, alteration, deletion, disclosure of data. General access to personal data is only possible to recipients with a UserID/Password. Physical copies of personal data are stored in a properly secured manner.

The contractor has signed a Data Processing Agreement committing to appropriate technical and organisational measures to ensure security of personal data and to comply with data protection requirements of European law.

Access to the system is via EULogin. EULogin requires a UserId/password and, when connecting from outside of the network of the EEAS, two-factor authentication. The EULogin privacy statement is available here: https://ecas.ec.europa.eu/cas/privacyStatement.html

9. EEAS DATA PROTECTION OFFICER: Any questions to the DPO?

If you have enquiries you can also contact the EEAS Data Protection Officer at data-protection@eeas.europa.eu.

10. RECOURSE

You have, at any time, the right to have recourse to the European Data Protection Supervisor at edps@edps.europa.eu.