Data protection statement on the processing of personal data relating to the Operational Usage of FIPS (SAP) / myFIPS in PD4.1 and PD4.7

Protecting your privacy is of the utmost importance to the European Patent Office (EPO). We are committed to protecting your personal data and ensuring respect for data subjects' rights when performing our tasks and providing our services. All data of a personal nature that identify you directly or indirectly will be processed lawfully, fairly and with due care.

The processing operations described below are subject to the EPO Data Protection Rules (DPR).

The information in this statement is provided in accordance with Articles 16 and 17 DPR.

In line with the Financial Regulations PD4.1 and PD4.7 process data available in FIPS in order to facilitate procurement processes and payment.

1. What is the nature and purpose of the processing operation?

The FIPS (SAP) system and myFIPS (online interface for FIPS) is used in Finance and Procurement to log and store all operational documents needed run the finance and procurement processes. Considering that SAP is an integrated system that covers also the HR part, this assessment will cover only the parts directly linked to the Procurement processes.
FIPS is used holistically for posting documents and includes documentation stored there from different applications in order to ensure full transparency of decision to all involved staff. Main processes covered there are Planning, Budgeting, Reservation of Funds, Sourcing, Contract management, Purchasing/ordering, Goods/Service Receipts, Invoicing, Payments, Cash Management, PSCD, Sales & revenue, Controlling, Master Data, Reporting, User management etc. All above mentioned processes involve most of the staff in EPO assigned to approve different stages of the process, reporting, controlling and operational activities. As a result, multiple information data sources are processed that are logged in the tool to ensure auditability and sound process control. The access to data is centrally managed on a need-to-know basis by the BIT colleagues responsible who are responsible to follow system and governance rules. On the operational tasks, colleagues themselves are responsible to add all information and files needed for internal approval and auditability of procurement postings.
Further to internal staff, some specific information (based on approved requests) is accessible to auditors, IT support staff (internal or external), consultants involved in projects, contract managers.

The processing is not intended to be used for any automated decision-making, including profiling.

Your personal data will not be transferred to recipients outside the EPO which are not covered by Article 8(1), (2) and (5) DPR unless an adequate level of protection is ensured. In the absence of an adequate level of protection, a transfer can only take place if appropriate safeguards have been put in place and enforceable data subject rights and effective legal remedies for data subjects are available, or if derogations for specific situations as per Article 10 DPR apply.

2. What personal data do we process

The categories of data subject concerned are EPO employees and employees of the external providers.

The categories of personal data processed might be:

- SAP Logs
- **Contact Information**: Contact Details, Country, Mobile Phone Number, Phone Numbers, Working email address
- **Correspondence** any Information which might be provided in the course of exchanges, Chat content, Personal information provided voluntarily
- **Education & Skill** (such as, education and Training History, educational Degrees, languages, project management experience
- **Employment Information** Business Unit Division, Company Entity, Department name and/or number, EPO access badge number, End Date, Job Title Role, Room Number
- **Financial information**
- **Personal Identification data**
- **System Log:** File data (name, size and/or hash, Registry data, SAP log
- **Ticketing information**
- **Contact Information** Contact Detail , Phone Number, Working email address
- **Physical and/or Digital Identifiable Assets,** such as the digital Certificate

Further to that the above, details for suppliers and bidders that participated in procurement procedures, together with the info on whether they were awarded any contracts.

3. Who is responsible for processing the data?

Personal data are processed under the responsibility of the Principal Director Procurement and Vendor Management of PD4.7 acting as the EPO's delegated data controller.

Personal data are processed by the EPO staff involved in managing the initiative, project or activity of PD4.1 and referred to in this statement.

4. Who has access to your personal data and to whom are they disclosed?

Personal data are disclosed on a need-to-know basis to all staff/consultants/auditors based on the roles given by the BIT team. Other parties will have access to aggregated operational data through reporting.

Personal data will only be shared with authorised persons responsible for the necessary processing operations. They will not be used for any other purposes or disclosed to any other recipients.

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

PD4.7 takes appropriate technical and organisational measures to safeguard and protect your personal data from accidental or unlawful destruction, loss or alteration and unauthorised disclosure or access.

All personal data are stored in secure IT applications in accordance with the EPO's security standards. Appropriate levels of access are granted individually only to the above-mentioned recipients.

All personal data included in FIPS/myFIPS is stored in secure IT applications and follow the BIT security standards in EPO. These include:

- User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication;
- Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum;
- Logical security hardening of systems, equipment and network: 802.1x for network access, encryption of endpoint devices, AV on all devices
- Physical protection: EPO access controls, additional access controls to datacentre, policies to lock offices;
- Security incidence response: 24/7 monitoring for incidents, on-call security expert.third-party certification.

In principle, the EPO has adopted a paperless policy management system; however, if paper files containing personal data need to be stored on EPO premises, they are locked in a secure location with a restricted access. When data are outsourced (e.g. stored, accessed and processed), a privacy and security risk assessment is carried out and the following general statement might be included in this field:

For personal data processed on systems not hosted on EPO premises, the providers processing the personal data have committed in a binding agreement to comply with their data protection obligations under the applicable data protection legal frameworks. The EPO has also carried out a privacy and security risk assessment. These systems are required to have implemented appropriate technical and organisational measures such as: physical security measures, access and storage control measures, securing data at rest (e.g. by encryption); user, transmission and input control measures (e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), audit logging); conveyance control measures (e.g. securing data in transit by encryption).

6. How can you access, rectify and receive your data, request that your data be erased, or restrict/object to processing? Can your rights be restricted?

You have the right to access, rectify and receive your personal data, not to be subject to a decision based solely on automated processing, to have your data erased and to restrict and/or object to the processing of your data (Articles 18 to 24 DPR).

If you would like to exercise any of these rights, please write to the delegated data controller at PDCProcuremet-dpl@epo.org. In order to enable us to respond more promptly and precisely, you always need to provide certain preliminary information with your request. We therefore encourage you to fill in this form (for externals) or this form (for internals) and submit it with your request.

We will reply to your request without undue delay and in any event within one month of receipt of the request. However, Article 15(2) DPR provides that this period may be extended by two further months where necessary in view of the complexity and number of requests received. We will inform you of any such delay.

7. What is the legal basis for processing your data?

Personal data are processed on the basis of Article 5 DPR (a), the processing is necessary for the management and functioning of the EPO, not all processing operations required for the functioning of the EPO are explicitly mandated by EPC.
In addition, personal data is collected and processed in accordance with the Financial Regulations (Budget Implementation Directive, Tender Guidelines, Directive on Contracts, Directive supplementing certain provisions of the Financial Regulations).

8. How long do we keep your data?

No data retention policy in place. There are predefined legal requirements regarding contracting and invoice postings. An archiving project is not yet put in place.

9. Contact information

If you have any questions about the processing of your personal data, please write to the delegated data controller at PDCProcurement-DPL@epo.org

You can also contact our Data Protection Officer at dpo@epo.org.

Review and legal redress
If you consider that the processing infringes your rights as a data subject, you have the right to request review by the controller under Article 49 DPR and, if you disagree with the outcome of the review, the right to seek legal redress under Article 50 DPR.