Data protection statement on the processing of personal data in the context of Splunk

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.

Splunk is the EPO's central log repository for security incident management enabling the protection of EPO systems by helping to identify and analyse security issues.

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

The processing of data using Splunk comprises the following:
- receiving technical data generated and already available from other BIT systems and services
- performing automated queries to generate alerts for relevant security events
- performing automated queries to generate dashboards and overviews of security-relevant information
- performing manual queries for deeper analysis of security events, adaptation of dashboards and alerts

Splunk receives technical data generated on (and available on) a number of EPO systems and services, in particular:
- EPO-managed workstations assigned to EPO users
- EPO-managed servers
- EPO-managed network equipment (e.g. routers, switches, firewalls and proxy servers)
- external cloud providers with an established contractual relationship with the EPO (e.g. Microsoft, Google, Amazon and SAP)

Personal data are processed for the purpose of identifying the persons who carried out the activities that have been logged, in order to address any possible error or security incident detected. This is important because:
- log files are used to trace events in an information system and to help debugging and repair. They are part of the system and essential to provide security and efficient support when information systems are not working correctly;
- log files of EPO systems are processed to investigate and resolve security incidents and malware infections on devices connected to the EPO network, and/or to prevent data leaks;
- additionally, log files may be processed for statistical purposes or to solve problems with users' access to EPO telecommunications systems.

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.

2. What personal data do we process?

Through Splunk the delegated controller, BIT PD 4.6, collects personal data, as and when such data are included in the logs generated by the origin system. No special categories of personal data are knowingly or willingly collected via Splunk.

Processed personal data may refer to EPO employees, EPO contractors or externals.

Processed personal data if the data subject is an EPO employee or a contractor:
- personal identification data: full name, (first name + last name) and gender
- contact information: email address at work, phone numbers

- user account information: userID, account number
- network/application interaction data: session metadata
- system logs: running processes, registry data, file metadata (file name, size, hash), port numbers, transaction-related details, audit logs, system-, application- and security-related server logs, web server logs, firewall/router/switch logs
- identifiers of physical/digital assets which the data subject used to connect to EPO systems: the serial number, hostname and operating system version of the workstation, the MAC address of the network interface
- browsing information: browser type, URL, browser user agent, browsing date and time, IP address, category, website history, network interaction history
- phone call information: caller number, called number, date and time, duration, interaction history
- telephony interaction data: telephony session metadata
- employment information: active/inactive indicator, end data, department name and/or number, room number, office location, job title, job group (only for employees), start date, line reporting manager, language preference (for communication), contract type, personnel number
- ticket-related data
- geolocation information

Processed personal data if the data subject is external:

- network/application interaction data: session metadata
- system logs: firewall/router/switch logs, web server logs, system, application and security-related server logs
- identifiers of physical/digital assets which the data subject used to connect to EPO systems: the hostname and operating system version of the workstation, the MAC address of the network interface
- browsing information: browser type, URL, browser user agent, browsing date and time, IP address, category, website history, network interaction history
- phone call information: caller number, called number, date and time, duration, interaction history
- telephony interaction data: telephony session metadata
- ticket-related data

3. Who is responsible for processing the data?

Splunk personal data are processed under the responsibility of CIO/BIT Principal Directorate 4.6, acting as the EPO delegated data controller.

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

Splunk personal data are only accessed by recipients in BIT departments 4623 Information Security and 4638 Network and Data Centre Management, for necessary processing operations.

All use of Splunk is to support security use cases by BIT Department 4623 Information Security and network-related use cases by BIT Department 4638 Network and Data Centre Management, in accordance with the need-to-know principle.

External contractors may occasionally process Splunk personal data (including accessing it) while providing Splunk software maintenance services.

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

We take 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 in scope of existing processing operations are stored within a secure, in-house IT application, in accordance with the EPO's Information Security Policy Framework.

Physical security: physical access controls are enforced at EPO office premises; additional access controls are enforced at the EPO data centres in Luxemburg and Munich.

Logical security: hardening is applied to systems, equipment and network.

Access control: role-based access control to the systems and network, in accordance with the need-to-know and least-privilege principles; segregation of administrative and user roles; reduction of overall administrative roles to a minimum.

Access to Splunk is role-based. Active Directory groups govern which roles are assigned to users, and roles are restricted in terms of the type of information they can access in Splunk. Appropriate levels of access are granted individually, and only to the above-mentioned recipients.

User authentication: all workstations and servers require login; mobile devices require login to the EPO enclave; privileged accounts require additional and stronger authentication. All queries using Splunk are performed by authenticated users. Authentication is based on the EPO Active Directory systems, thereby ensuring that regular account lifecycle management is implemented (e.g. deactivation of accounts for staff no longer in service).

Logging: Splunk maintains a full audit trail of user queries and other activity. This information, like any other information in Splunk, is “append only”, meaning that once entered it cannot be altered or removed undetected.

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 DP_BIT@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(a) DPR: processing is necessary for the performance of a task carried out in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office’s management and functioning.

Personal data are processed on the basis of the following legal instrument: Article 7 “Monitoring, controls, audits and further processing” of Circular 382 (29 March 2017) EPO Information Security Guidelines.

8. For how long do we keep your data?

Splunk personal data will be kept only for the time needed to achieve the purposes for which they are processed.

Data stored in Splunk on-premise are subject to the regular backup and archiving retention policy for on-premise servers.

Splunk log files are stored automatically and are kept for an agreed period of time depending on the type of information and the system to which they refer. Microsoft Defender for Endpoint Security alert/incident-related data are retained for 12 months within Splunk. Other data are kept in Splunk for up to 18 months, after which they are automatically deleted. Data are kept in backups for 60 days after removal from the Splunk system, after which they are no longer available. This means that Splunk's overall data retention never exceeds 20 months.

In the event of a formal appeal/litigation, all data held at the time the formal appeal/litigation was initiated will be retained until the proceedings have been closed.

9. Contact information

If you have any questions about the processing of your personal data, please write to the delegated data controller at DP_BIT@epo.org for EPO staff members, or to DPOexternalusers@epo.org for external data subjects.

Internals may also contact our Data Protection Officer at dpo@epo.org, while externals may contact our Data Protection Officer at DPOexternalusers@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.