Data protection statement on the processing of personal data in Okta's Customer Identity and Access Management (CIAM) system

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.

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

This data protection statement relates to the processing of personal data in Okta. The EPO uses Okta's cloud-based software as a service (SaaS) platform for the purpose of Identity and Access management.

The processing operation involves user authentication via Okta. The authentication is required as soon as you attempt to log in to a secure area of EPO online services that is accessible with a smart card or with account credentials obtained for using those services.

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.

2. What personal data do we process?

The following categories of personal data are processed:

- first and last name
- smart card number
- preferred language
- email address
- username
- password
- phone number
- connection/localisation data

3. Who is responsible for processing the data?

Personal data are processed under the responsibility of the EPO Principal Directorate CIO acting as the EPO's delegated data controller.

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

The personal data are disclosed on a need-to-know basis to the EPO staff (system administrators) of the Information Security Dept. 4.6.2.3 and to some EPO staff of DG1 for customer support purposes. They are also disclosed on a need-to-know basis to Okta's staff for maintenance and support purposes. 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?

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.

For personal data processed on systems not hosted on EPO premises, Okta has 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.

Okta does not transfer the personal data to countries that do not guarantee adequate levels of data protection.

Okta has administrative, physical and technical safeguards in place to protect the security, confidentiality and integrity of both customer and personal data. These safeguards are described in Okta's trust and compliance documentation.

Okta has obtained certification under the Asia-Pacific Economic Cooperation scheme of Privacy Recognition for Processors and processes personal data accordingly.

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 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 in accordance with Article 5(a) DPR, which provides for processing which "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".

8. How long do we keep your data?

Personal data processed by the delegated data controller or the service providers under its supervision are stored for no longer than necessary for the purposes for which it has been processed.

Personal data will be stored for the duration of the contract with Okta.

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.

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 delegated data 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.