

Effective from May 1, 2025

1. Home

Purpose of the Policy. This personal data processing policy ("**Policy**") governs the conditions under which personal data is processed and sets out the rights and obligations of the data controller and data subjects. They also define the legal titles for processing and the conditions under which personal data may be transferred to other entities. All processing of personal data is carried out in accordance with the European Union General Data Protection Regulation 2016/679 ("**GDPR**").

The Controller. The Controller is **SEFIRA spol. s r.o.**, with its registered office at Prague 4 - Krč, Antala Staška 2027/77, Postal Code 14000, ID No.: 629 07 760, registered in the Commercial Register at the Municipal Court in Prague under No. C 34572 ("**Controller**" or "**SEFIRA**").

Data subject. The Policy applies to situations where the Controller processes your personal data as a data controller and is therefore responsible for the processing of your personal data. This applies to the following situations:

- **Signature of the Agreement.** The Controller processes the personal data of whoever acts on behalf of your company (e.g. an executive) in connection with the negotiation and conclusion of the Agreement.
- **Performance of the Agreement.** In addition, the Controller processes personal data of your employees, external collaborators or anyone else acting on behalf of your company or using the Services for work (collectively, "**Employees**") for the purpose of providing performance under the Agreement (the Controller records the Account controller's data).
- **Development Services.** After the conclusion of the Agreement, during the provision of the Services, the Controller may process personal data, for example, for the purpose of analyzing and optimizing the provision of the Services.

Conditions. The content of the Agreement is governed by the Obelisk Cloud Services Terms of Use ("**Terms**"). Capitalized terms not defined in the Policies shall have the meanings set forth in the Terms.

Scope of processing. The Controller shall process personal data to the smallest possible extent. The processing of personal data is necessary in certain cases, in particular for the purposes of concluding the Agreement and the proper provision of the Services.

SEFIRA as a processor of personal data. Because in the course of using the Services you may disclose to the Controller the personal data of your customers, potential customers or your other employees and associates (e.g. those who do not use the Services and are therefore not "**Employees**" as defined above), in relation to your customers you are the data controller and SEFIRA is the data processor, or you are the processor and SEFIRA is another processor. However, such relationship is not subject to this Policy. For this purpose, there is a separate agreement on the processing of personal data, which is an integral part of the Policy.

Contact details. The Controller can be contacted using the following details:

E-mail: gdpr@sefira.com

Phone: +420 222 558 111

2. Personal data

The data processed and the purpose of their processing can be divided into the following categories:

- **Identification data.** For example, name and surname and/or business name, date of birth, identification number and address of registered office or residence or other identifying information.
- **Contact details.** For the purpose of being able to contact you or an Employee in connection with the Agreement and the provision of the Services or with a commercial communication. This includes telephone and email address.
- **Login details.** For the purpose of logging Employees into Accounts. This includes username and password or other means.
- **Information about your device.** In order to ensure the proper provision of the Services and the proper operation of the Website or Customer Portal. For this purpose, the Controller of also processes cookies. This includes, for example, IP address, operating system version, browser type, location and other data provided.

- **Billing and bank details.** In connection with the identification and execution of payments. This includes, for example, information appearing on invoices, bank details and information about payments received or sent.
- **Information from our communication.** In particular, information in emails, records of telephone calls or information contained in contact forms and the content of communications with the Controller. This may include, for example, job titles or other personal information that you or the Employee disclose to the Controller.

3. Reason and time of processing

The Controller is authorized to process personal data only on the basis of a relevant legal title supported by applicable law. The Controller processes personal data solely on the basis of the following legal titles:

Legal basis for processing under the GDPR	Reason for processing	Processing time	Personal data processed
AGREEMENT performance of obligations under the contract or in pre-contractual negotiations <i>Article 6(1)(b) GDPR</i>	In the case of negotiations for the conclusion of the Agreement or in the case of the conclusion of the Agreement , the Controller processes the personal data of certain persons in your company (e.g. the managing director or other signatory, the Account administrator). The Controller also needs the data during the performance of the Agreement (e.g. communication with the Controller regarding a query or error in the provision of the Services).	For the duration of the Agreement .	Identification data Contact details Login details Information about your device Billing and bank details Information from our communication
LEGAL OBLIGATION the fulfilment of obligations arising from legal regulations <i>Article 6(1)(c) GDPR</i>	The Controller processes personal data if it is required to do so by law , in particular accounting and tax law.	For the period required by the law (usually for 10 years from the end of the financial year in which the tax/accounting event occurred)	Identification data Contact details Billing and bank details
LEGITIMATE INTEREST it is in the legitimate interest of the Controller <i>Article 6(1)(f) GDPR</i>	In order to protect against attacks, spam or other damage , the Controller may process log files, including the IP address of the accessing person, as part of the access to the provision of the Services.	For a maximum period of 3 months from any activity within the use of the Services .	Information about your device

	For the purpose of sending newsletters to its customers , for example, with information regarding the provision of the Services.	For a period of 3 years from the end of the Agreement , or until you object to this processing, e.g. by unsubscribing from the newsletters.	Identification data Contact details
	For the purpose of informing you of important matters relating to the provision of the Services (e.g. downtime).	For the duration of the Agreement.	Identification data Contact details
	For the purpose of protecting its rights and legally protected interests (e.g. in the event of a dispute arising in connection with the Agreement).	For a maximum period of 16 years from the end of the Agreement . This corresponds to the maximum limitation period under the Civil Code (15 years) plus 1 year for situations where we receive a claim from you after the limitation period has expired.	Identification data Contact details Billing and bank details Information from our communication
CONSENT the data are processed by the Controller on the basis of the data subject's consent <i>Article 6(1)(a) GDPR</i>	For the purpose of processing data that cannot be classified under any of the above legal grounds.	During the period of consent. Consent to the processing of personal data can be withdrawn at any time, for example by e-mail. However, the withdrawal of consent or its expiry does not imply an obligation on the part of the Controller to delete all data, provided that there is another legal basis for further processing. Withdrawal of consent does not affect the lawfulness of previous processing.	The data that are included in the consent to the processing of personal data.

The Controller processes personal data manually and with the use of automated processing, however, it will not carry out profiling.

4. Data processors

The Controller also transfers personal data to other entities that are in the position of personal data processors. They are entitled to process the personal data transferred only within the agreed scope.

Specifically, the Controller transfers processed personal data to the following entities:

- Amazon Web Services, a cloud solution provider;
- Bankovní identita, a.s., operating the Bank iD service;
- První certifikační autorita, a.s., provider of electronic identification services;
- partners who provide certain other services to the Controller (e.g. providers of accounting, tax or legal advice; auditors; CRM solution provider; senders of commercial communications, etc.).

The Controller may transmit personal data to public authorities if requested to do so or if it is in the controller's interest to do so.

5. Transmission of personal data

The Controller does not transfer personal data outside the EU. The Controller should decide to transfer personal data outside the EU in the future, it will only do so in accordance with the GDPR and only to countries or entities where an adequate level of data protection is ensured. In the case of transfers to third countries, such transfers will only be made on the basis of standard contractual clauses approved by the European Commission. Personal data will only be transferred to companies that are committed to complying with the European Commission's data protection requirements.

6. Rights of data subjects

You have the following rights in relation to the processing of personal data. You can exercise them via letter to the address of the Controller's registered office, via e-mail to gdpr@sefira.com or via electronic data mailbox (ID: ts8zphg).

- **Right to withdraw consent.** If the Controller processes personal data on the basis of your consent, you can withdraw it at any time.
- **Right of access.** You have the right to obtain information about what data the Controller holds about you and how it processes that data. Also, you have the right to access this personal data or a copy of it. The Controller will provide you with the first copy free of charge; for the second and subsequent copies, the Controller is entitled to claim reimbursement of the necessary costs of making the copy.
- **Right to rectification and completion.** If you discover that the Controller is processing incorrect data, you have the right to request its correction or completion.
- **Right to erasure.** Under certain conditions, the Controller is also obliged to delete the personal data it holds about you. For example, if there is no longer any reason on its part to process the personal data for the purposes for which it was collected or in connection with compliance with another request from you (withdrawal of consent, objection).
- **Right to restriction of processing.** If you do not wish to have your personal data erased but do not wish the Controller to continue to process it, you can ask the Controller to restrict the processing of your personal data.
- **Right to portability of personal data.** In some cases, you may ask the Controller to transfer the personal data it holds about you to you or another responsible person in a structured, commonly used and machine-readable format.
- **Right to object.** You also have the right to object (in the case of processing based on legitimate interest). The Controller will then evaluate the objection within one month of receipt. In the event of an objection to the further transmission of commercial communications, the Controller will always comply with the objection.
- **Right to lodge a complaint.** If you suspect that your personal data is being unlawfully processed, you may file a complaint with the Office for Personal Data Protection, <http://www.uoou.gov.cz/> Pplk. Sochora 27, 170 00 Prague 7.