Data processing agreement

sefira

Effective from May 1, 2025

1. Introduction and purpose of this DPA

1.1. **Cooperation.** The Provider and the Customer have entered into an Agreement under which the Customer uses the Services. In connection with the Agreement, the Provider may in certain cases process personal data of the Customer's employees, persons acting on behalf of the Customer (e.g. managing director) and other associates (e.g. Account administrator). For the sake of simplicity, this document uses the term **"Employees"** to refer to all such persons. At the same time, the Provider also processes the personal data of the Customer's Clients, if such data is processed within the scope of the Services. For the purposes of this document, the term **"Clients"** will be used to refer to such persons.

1.2. **Subject of the DPA.** This document serves as a personal data processing agreement (**"DPA"**) that must be concluded between the controller and the processor of personal data pursuant to Article 28 of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (**"GDPR"**).

1.3. **Terms.** This DPA is an integral part of the Obelisk Cloud Services Terms of Use (**"Terms"**). Capitalized terms used in this DPA have the same meaning as in the Terms or Agreement.

1.4. **Controller or processor.** The Customer is the controller of personal data. In the course of its business activities, it processes the personal data of Employees and Clients. The Provider is the processor of personal data. Based on this DPA, the Customer's instructions, and the Customer's use of the Services, the Provider will process the personal data of Employees and Clients in connection with the use of the Services for the Customer.

1.5. **Provider as controller.** In relation to certain personal data of the Customer or its Employees, the Provider may also be the controller. This situation is governed by the Personal Data Processing Policy available at https://www.sefira.com/en/ke-stazeni/.

1.6. **Customer Responsibility.** The scope of processing is always determined exclusively by the Customer, who is also responsible for ensuring that the specified scope of processing complies with the GDPR and Act No. 110/2019 Coll., on the processing of personal data. The Customer declares that the data made available to the Provider in connection with the use of the Services is managed in accordance with the regulations and that the Customer fulfills all obligations of the controller in accordance with the currently effective regulations.

1.7. **Authorization of the Provider.** The Customer, as the Provider's controller within the meaning of Article 28 of the GDPR, authorizes the processing of personal data in accordance with this DPA.

2. Access to data and reason for processing

2.1. **Personal data.** The subject of processing is personal data of data subjects provided by the Customer when using the Services, and any other data provided by third parties based on the Customer's instructions.

2.2. **Personal data of Employees.** When providing Services to the Customer, the Provider processes the personal data of Employees. The Provider may obtain access to this personal data in three ways:

2.2.1. **Use of the Services by the Employee.** In order for the Employee to have an Account to use the Services, the Provider needs the Employee's personal data to set up the Account (or has access to this data when the Customer sets up the Account themselves and thereby makes the personal data available to the Provider).

2.2.2. **Storage of Employee data.** If the Customer or its Employee stores data of another Employee while using the Services, the Provider will process that data.

2.3. **Specific Employee Data.** In order for an Employee to use the Services within the meaning of paragraph 2.2.1, the Customer shall provide the Provider with at least the following data.

2.3.1. **Identification data** (e.g., name and surname);

2.3.2. **Contact details** (e.g., e-mail and telephone number);

2.3.3. **Login details** (e.g., Customer name and password);

2.3.4. **Information about the Employee's job classification** (e.g., job position, role)

2.3.5. **Other data provided by the Customer or Employee when using the Services or during mutual communication** (e.g., other data according to the functions made available and used when using the Services).

2.4. **Purpose of processing.** The Provider processes the personal data of Employees for the purpose of providing the Services under the Agreement and for the purpose of communicating with Employees if they contact the Provider.

2.5. **Personal data of Clients.** When providing the Services, the Provider processes not only the personal data of Employees, but also the personal data of the Customer's Clients. In general, the following personal data will be processed:

2.5.1. **Identification data** (e.g., name and surname, name of the company, identification number)

2.5.2. **Contact details** (e.g., e-mail, telephone number)

2.5.3. **Adress details** (address)

2.5.4. **Information relevant for the Customer's business** (e.g., service provided to Client, its status, etc.)

2.5.5. **Billing and bank details** (e.g., information appearing on invoices, bank details, and information about payments received or sent);

2.5.6. **Other data provided by the Customer or Employee when using the Services or during communication with the Provider** (e.g., information contained in uploaded documents, information about electronic signatures, information about the use of the Services).

2.6. **Purpose of processing.** The Provider may process Clients' personal data for the purpose of providing the Services under the Agreement.

3. Methods of processing

3.1. **Nature of personal data processing.** The processing of personal data by the Provider may involve collecting, recording, storage on information carriers, sorting, transfer, and retention, as well as other activities necessary for the performance of the Agreement, either automatically or manually, in such a way that these activities correspond to the purpose of personal data processing.

3.2. **Responsibility of the Provider.** The Provider is responsible for ensuring that it complies with DPA and the Customer's instructions during processing and that it processes personal data only in accordance with the applicable legal regulations.

3.3. **Instructions.** The processing of personal data is carried out on the basis of instructions from the Customer, as the controller. The main instructions for processing are this DPA, Terms, the Agreement, and, where applicable, the activities performed by the Customer and/or Employees in connection with the use of the Services. If additional Instructions are provided, the Customer must submit them in writing to gdpr@sefira.com. If the Provider finds that the Customer's instruction violates legal regulations, it shall inform the Customer thereof without undue delay. If the Customer insists on the instruction or fails to remedy the defect, the Provider is entitled to withdraw from the Agreement and shall not be liable for any damage caused by such instruction.

4. Other important information

4.1. **Processing period.** The Provider shall process the personal data of Employees and Clients for the duration of the Agreement, unless otherwise specified in this DPA. If the Customer deletes their data earlier, the Provider shall terminate their processing without undue delay after their deletion. Furthermore, paragraph 4.2 shall apply.

4.2. **Termination of cooperation.** Upon termination of cooperation, the Customer may download the data on Employees and Clients in a machine-readable format no later than 30 days after the termination of the Agreement. The Provider shall, for its part, demonstrably delete all personal data from all storage locations no later than 60 days after the end of the processing period, unless it is required or permitted by law to continue processing certain data.

4.3. **Storage location.** All personal data is stored by the Provider within the EU.

4.4. **Security measures.** The Provider undertakes to take the necessary technical, organizational, and other measures to ensure the protection of personal data so that unauthorized or accidental access to personal data, its alteration, destruction, loss, unauthorized transfer, or other misuse cannot occur. An overview of the measures is provided in Section 4.10 of this DPA.

4.5. **Transfer of personal data.** When processing personal data, the Provider may use other processors **("Subprocessors"**). These are providers who are involved in providing the Provider's services (primarily hosting or IT service providers) and are not employees of the Provider (e.g., self-employed contractors). At the same time, the Provider uses suppliers who may have access to personal data as Subprocessors. These may include, for example, providers of cloud and other storage or other software necessary for the provision of the Services. The Customer grants general permission to involve these Subprocessors. The Provider shall inform the Customer of any changes relating to Subprocessors, including their acceptance or replacement. The Customer is entitled to raise objections within 14 days of notification, but undertakes not to do so without just reason. The list of Subprocessors as of the date of signing the Agreement is as follows:

4.5.1. Amazon Web Services, cloud solution provider;

4.5.2. Bankovní identita, a.s., operating the Bank iD service;

4.5.3. První certifikační autorita, a.s., provider of electronic identification services;

4.5.4. partners who provide certain additional services to the Provider (e.g., accounting, tax, or legal advisors; auditors; CRM solution providers; distributors of commercial communications, etc.).

4.6. **Obligations of the Subprocessor.** If the Provider engages a Subprocessor, it shall impose on the Subprocessor at least the same obligations as those set out in this DPA. It shall require the Subprocessor to comply with the GDPR and to protect the personal data transferred using adequate security measures.

4.7. **Cooperation.** The Provider shall cooperate in ensuring compliance with the obligations under Articles 32 to 36 of the GDPR in relation to Employees and Clients, taking into account the information available to it. If any of your Employees or Clients contact the Provider and exercise their rights relating to the processing of personal data, the Customer shall forward such request to the Provider without undue delay for resolution.

4.8. **Confidentiality.** The Provider shall maintain confidentiality regarding all personal data and other information that it learns during the processing of personal data. It shall handle such data only to the extent and to the degree necessary to fulfill the Agreement, this DPA, and the stated purposes of processing. The Provider's employees and associates are properly trained in the handling of personal data and will also maintain its confidentiality and secrecy, as well as comply with all measures required by Article 32 of the GDPR regarding the security of personal data entrusted for processing.

4.9. **Audits.** At the Customer's request, the Provider shall provide all information necessary to demonstrate that the obligations laid down in Article 28 of the GDPR have been fulfilled and shall allow the Customer or a third party to conduct an audit to a reasonable extent, no more than once every two years and after prior written notice of at least 30 days. The Provider is entitled to reject the date proposed by the Customer and propose an alternative date, which must not be later than 30 days after the date originally proposed by you. The costs of the audit shall be borne by the Customer. The Customer is also obliged to maintain confidentiality regarding all information obtained during the audit concerning the Provider, in particular its security policies and standards. The Customer is obliged to impose the same obligation on third parties entrusted by it to carry out the audit.

4.10. **Measures.** In order to fulfill its obligations, taking into account the state of the art, the costs of implementation, the nature, scope, context, and purposes of processing, as well as the varying likelihood and severity of the risks to the rights and freedoms of natural persons, the Provider undertakes to ensure data processing at least in the following manner:

4.10.1. uses secure storage and access to Services and other systems, where access will be known only to the necessary extent of employees and associates;

4.10.2. uses secure access to administration or other personal data databases;

4.10.3. uses software and services that meet standard data security requirements for the processing of personal data;

4.10.4. without the prior consent of the Customer, the Provider shall not make copies of the personal data database, except for necessary technical backups;

4.10.5. uses appropriate security measures, such as encryption or other appropriate and necessary measures, always depending on the specific action and data;

4.10.6. not allow access to personal data to third parties unless such access is approved in writing by the Customer or unless it follows from the Agreement;

4.10.7. processes personal data in the form in which it was provided by the Customer;

4.10.8. processes personal data only for the purposes specified in this DPA and to the extent necessary to fulfill these purposes.

4.11. **Notification of a security incident.** If the Provider discovers that a security incident and breach of personal data processing has occurred during the provision of Services and handling of personal data on the part of the Provider, it shall notify the Customer without undue delay.

5. Conclusion

5.1. **Changes of the DPA.** In the event of a change to the DPA, the Provider shall inform the Customer of the change in advance. If the Customer believes that the change leads to a violation of the GDPR or other legal regulations, they are obliged to inform the Provider and are entitled to reject such a change. The Provider shall then make the necessary adjustments to remedy the situation.

5.2. **Effectiveness of the DPA.** This DPA shall become effective for the Customer upon approval of the Terms or upon signing a separate Agreement. They shall also apply to services provided prior to that date.