Exoscale Data Processing Addendum

This Data Processing Addendum (referred to as the "Agreement") forms part of the Contract for Services under Exoscale's Terms and Conditions and/or Exoscale's End User Service Agreement (both referred to as the "Principal Agreements") between Akenes SA (referred to as the "**Processor**") and the "**Company**" using Exoscale's services.

Exoscale is a registered trademark of the Processor Akenes SA, Boulevard de Grancy 19A, 1006 Lausanne, Switzerland, company identification number CHE-423.524.322.

This Agreement governs the specific requirements of Data Protection Laws to the extent that Company's use of Exoscale's Services implies the processing of Personal Data subject to Data Protection Laws.

The terms of this Agreement shall follow the terms of the Principal Agreements. Terms not defined herein shall have the meaning as set forth in the Principal Agreements.

This Agreement is applicable starting May 5th, 2025, and binding at Company's acceptance date, as stored in the legal section of Company's account at Exoscale.

WHEREAS

1. The Company acts as a Data Controller (the "Controller").

2. The Company wishes to subcontract certain Services (as defined below), which imply the processing of Personal Data, to Exoscale, acting as a Data Processor (the "Processor").

3. The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) and the Swiss Federal Act on Data Protection of 25 September 2020 (FADP; RS 235.1) and other applicable data protection laws.

4. The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation

Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

1. "**Agreement**" means this Data Processing Addendum and all Schedules;

2. "**Company Data**" means any data (including but not limited to any software application) stored by Company on the cloud infrastructure provided by Processor, including all text, pictures, sound, video, and log files and all documentation (printed or electronic).

3. "**Company Personal Data**" means any Personal Data related to the Company or Company's customers or employees processed in connection with the Principal Agreements;

4. "**Contracted Processor**" means a Subprocessor;

5. “**Data Protection Laws**” means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

6. “**EEA**” means the European Economic Area;

7. “**EU Data Protection Laws**” means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State, and as amended, replaced, or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

8. “**GDPR**” means EU General Data Protection Regulation 2016/679;

9. “**FADP**” means Federal Act on Data Protection of the 25th of September 2020 (FADP; RS 235.1)

10. “**Data Transfer**” means a transfer of Company Personal Data from Controller to the Processor or a Contracted Processor; or an onward transfer of Company Personal Data from the Processor to a Contracted Processor, or between two establishments of Processor or Contracted Processor;

11. “**Services**” means online services provided by the Processor, as described at Exoscale’s Website, consumed by Company excluding third Party services available from the Exoscale’s Marketplace. The purpose is the provision of the Services initiated by Company;

12. “**Subprocessor**” means any person appointed by or on behalf of Processor to process Personal Data on behalf of Controller in connection with the Agreement.

The terms “Commission”, “Controller”, “Data Subject”, “Member State”, “Personal Data”, “Personal Data Breach”, “Processing”, “Processor”, and “Supervisory Authority” shall have the same meaning as in the GDPR or other applicable Data Protection Law, and their cognate terms shall be construed accordingly.

2. Processing of Company Personal Data

2.1. Processor obligations

Processor shall:

1. comply with all applicable Data Protection Laws in the Processing of Company Personal Data;

2. not process Company Personal Data other than on Controller’s documented instructions.

2.2 Controller instructions

Controller instructs Processor to process Company Personal Data to:

1. provide the Services and related technical support;

2. fulfil legal obligations or resolve disputes;

3. exercise any internal task aimed to optimize the security, privacy, confidentiality, and functionalities of the Services;

4. exercise internal reporting, financial reporting, and other similar internal tasks.

3. Processor Personnel

Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know/access the relevant Company Personal Data, as strictly necessary for the purposes of the Principal Agreements, and/or to comply with Data Protection Laws and other relevant legislation, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1. Technical and Organizational measures

In accordance with Article 32 (1) of the GDPR, the Processor shall implement technical and organizational measures to ensure a level of security appropriate to the risk, considering the state of the art, the costs of implementation, and the nature, scope, context, and purposes of Processing, to protect the rights and freedoms of natural persons, and minimize the risk of a Personal Data Breach.

These measures include:

1. the pseudonymization and encryption of Company Data;

2. the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of Processing Services;

3. the ability to restore the availability and access to Company Personal Data in a timely manner in the event of a physical or technical incident;

4. a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

4.2. Certifications

The Processor continues to adjust technical and organizational measures to follow latest versions of security frameworks and comply with most recent revisions of internationally recognized security and privacy certifications as found at https://www.exoscale.com/compliance. These certifications are to demonstrate compliance with the requirements set out in section 4.1 of this Agreement.

5. Subprocessing

5.1. Appointment of Subprocessors

Processor shall not appoint (or disclose any Company Personal Data to) any Subprocessor unless authorized by the Company. The Company acknowledges and approves the following list of Subprocessors:

Name of Contracted Processor	Purpose	Location
Aiven Oy	Orchestration of Database as a Service (DbaaS) instances running on Processor’s infrastructure as Exoscale Services.	Helsinki, Finland

Company understands that this list may be updated by Processor regularly. Processor informs Company of any intended changes concerning the addition or replacement of other Processors at least 30 (thirty) days in advance. If Company objects the addition or replacement of a Subprocessor, it may terminate the Services upon 30 (thirty) days notice.

5.2. Agreements with Subprocessors

Processor ensures that Subprocessors are subject to an agreement with Processor no less restrictive and protective than the present Agreement with respect to the protection of Company Personal Data to the extent applicable to the nature of the Services provided by the Subprocessor.

Processor remains fully responsible towards the Controller for the fulfillment of obligations of the Subprocessors regarding Personal Data Protection.

6. Data Subject Rights

Considering the nature of the Processing, Processor shall assist Company for the fulfilment of Company's obligations to respond to requests to exercise Data Subject rights under applicable Data Protection Laws.

Processor shall:

1. promptly notify Company if it receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and

2. ensure that it does not respond to that request except on the documented instructions of Controller or as required by applicable laws to which the Processor is subject, in which case Processor shall to the extent permitted by applicable laws inform Controller of that legal requirement before the Contracted Processor responds to the request.

7. Personal Data Breach

7.1. Data breach process

The Processor shall manage any Personal Data Breach in compliance with applicable Data Protection Laws and its internal Personal Data Breach procedures. In the event of a Personal Data Breach affecting Company Personal Data, the Processor shall notify the Company without delay, providing sufficient information to enable the Company to fulfill its obligations under Data Protection Laws, including informing Data Subjects, as necessary. In such cases, the Processor shall provide the Company with sufficient information to allow the Company to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2. Co-operation

Processor shall co-operate with the Company and take reasonable commercial steps as directed by the Company to assist in the investigation, mitigation, and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

Processor shall provide reasonable assistance to Company with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data, and taking into account the nature of the Processing and information available to the Contracted Processors.

9. Deletion or Return of Company Personal Data

9.1. Service termination

In case of cessation of any Service involving the Processing of Company Personal Data, the Processor shall delete all Company Personal Data. Should the Company require a copy of their data, they must request it before the deletion of their account; requests made after the account has been deleted can no longer be considered.

9.2. Data return

Upon request of Company, notified at least 30 (thirty) days prior to termination of the Services, Processor shall make Company Data available to Company in its original format.

9.3. Deletion

Unless a request for the Processor's recovery service is made, Processor shall have no obligation to maintain or provide any of Company Data after termination of the Services and shall thereafter, unless legally prohibited, promptly and in any event within 10 (ten) business days of the date of cessation of any Services involving the Processing of Company Personal Data (the "Cessation Date"), delete and procure the deletion of all copies of those Company Personal Data.

10. Audit Rights

10.1. Audit process

Subject to this section 10, Processor shall make available to Company on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by Company or an auditor mandated by Company in relation to the Processing of the Company Personal Data by the Contracted Processors. Company shall not exercise its audit rights more than once per calendar year except following a Personal Data Breach or an instruction by a regulatory authority. Company shall give Processor at least 30 (thirty) days prior written notice of its intention to audit Processor pursuant to this Agreement.

10.2. Limitations

Audit shall be conducted during Processor's business hours, shall not disrupt Processor's operations, and shall ensure the protection of the Company's, Processor's, and other Data Subjects' Personal Data. Processor and Company shall mutually agree in advance on the date, scope, duration, and security and confidentiality controls applicable to the audit. Company acknowledges that signing a non-disclosure agreement may be required by the Controller prior to the audit.

10.3. Scope

Information and audit rights of Company only arise under section 10 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

11. Data Transfer

11.1. Data transfer between countries

Processor shall not transfer any Company Data, including Company Personal Data, between countries unless authorized by Company.

11.2. Data protection across jurisdictions

Processor shall only transfer or authorize the transfer of Data within Switzerland, the EU, the EEA, and/or countries subject to an adequacy decision, as provided for in art. 45 GDPR and art. 16 Swiss FADP. If Personal Data processed under this Agreement is transferred from Switzerland or any country within the EU, the EEA, or any country subject to an adequacy decision to a country outside of this scope, the Parties shall ensure that the Personal Data is adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on Switzerland- and/or EU- and/or EEA-approved and then-current standard contractual clauses for the transfer of Personal Data or other transfer mechanisms as provided by Data Protection Laws. Processor shall be authorized to perform such transfers to Subprocessors provided that adequate safeguards are implemented in regard to the nature of the transfer.

12. General Terms

12.1. Compliance with Applicable Laws

Processor will process Company Personal Data in accordance with this Agreement and Data Protection Laws applicable to its role under this Agreement. Processor is not responsible nor liable for complying with Data Protection Laws solely applicable to Company by virtue of its business or industry.

12.2. Confidentiality

Each Party must keep any information it receives about the other Party and its business in connection with this Agreement (“Confidential Information”) confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

1. disclosure is required by law;

2. the relevant information is already in the public domain through no fault of the Parties.

12.3. Notices

All notices and communications given under this Agreement must be in writing and will be sent by email. Controller shall be notified by email sent to the address related to its use of the Services under the Principal Agreements. Processor shall be notified by email sent to the address: privacy@exoscale.com.

12.4. Governing Law and Jurisdiction

This Agreement shall be governed by Swiss law, without regard to the choice or conflicts of law provisions of any jurisdiction to the contrary, and disputes, actions, claims or causes of action arising out of or in connection with this Agreement, an order form, any document incorporated by reference, Exoscale technology, or the Services shall be subject to the exclusive jurisdiction of Switzerland, specifically within the canton of Vaud (French: Canton de Vaud). It is governed by Swiss federal laws as well as the laws and regulations of the canton of Vaud.