Data Processing Agreement

BETWEEN:

anykey IT AG, located at Chriesbaumstrasse 2, 8604 Volketswil and represented by Tobias Linder, Chief technology officer;

Hereinafter, the "**Controller**".

AND:

Odoo SA, located in Chaussée de Namur 40, 1367 Ramillies, Belgium, registered in Belgium at the Crossroads Bank for Enterprises under number 0477.472.701, and represented by Sébastien Bruyr, Chief Commercial Officer;

Hereinafter, the "**Processor**".

The Controller and the Processor being hereafter referred to collectively as the "**Parties**" and any of them individually as a "**Party**".

1. Purpose

The purpose of this Agreement is to define the conditions in which the Processor undertakes to carry out, on the Controller's behalf, the personal data processing operations defined below. As part of their contractual relations, the Parties shall undertake to comply with the applicable Regulations on personal data processing (hereinafter the "***Regulations***") and including, in particular, 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, which is applicable from 25 May 2018 (hereinafter the "***GDPR***").

2. Duration of the Agreement

This Agreement is related to the Odoo Enterprise Agreement (hereafter, the "***Main Agreement***") signed between the Controller and the Processor. The duration of this Agreement will be the same as the Main Agreement.

3. Processor's obligations

The Processor shall undertake to:

a) Process personal data only for the purpose(s) that is/are the subject of the processing;

S.B.I.

b) Comply with the Regulations, and in particular to process personal data exclusively on the basis of documented instructions from the Controller;
c) Refrain from acting in a manner that would constitute or result in a violation of the Regulations by the Controller and immediately inform the Controller when the Processor believes that an instruction is being taken in violation of the Regulations.
d) If the Processor is required to transfer data to a third country or to an international organisation under the law of the European Union or the law of the Member State to which it is subject, it must inform the Controller of this legal obligation before processing, unless the relevant law prohibits such information for important reasons of public interest.
e) Guarantee the confidentiality of the personal data it receives from the Controller. The Processor can derogate from this obligation of confidentiality when a legal prescription or a judicial injunction obliges it to communicate the personal data or when the transfer of personal data takes place on the instructions of the Controller. Any legally binding disclosure of personal data to third parties must be notified in advance by the Processor to the Controller. Confidentiality will remain in place after the transfer or expiry of this Agreement.
f) The Processor also ensures that the persons authorized to process personal data under this Agreement: (i) undertake to respect confidentiality or are subject to an appropriate legal obligation of confidentiality; and (ii) receive the necessary information regarding the protection of personal data.
g) Satisfy its obligation to help the Controller, as far as possible, to follow up on requests relating to the rights of the data subjects.
h) If necessary, keep a record of the processing of activities carried out on behalf of the Controller. The Processor makes the register available to the Supervisory Authority on request.
i) If the Processor ascertains that Controller's instructions are contrary to the Regulations, it will immediately inform the Controller and may refuse to comply with such instructions until they comply with the Regulations.

4. Sub-contracting

In order to perform its obligations under the Main Agreement, the Processor may use third-party service providers (hereafter, the "***Subprocessors***") to process personal data.

a. Information about the Subprocessors, including their purpose and compliance policies, is available on the Processor Privacy Policy at https://www.odoo.com/privacy and updated by the Processor from time to time in compliance with this Agreement.
b. When engaging any Subprocessor, the Processor shall update the Odoo Privacy Policy mentioned in clause "a", before the Subprocessor begins processing any personal data.
c. When engaging any Subprocessor, the Processor will ensure via written contract that the Subprocessor only accesses and uses Controller data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the Main Agreement (including this Agreement). The Processor shall remain liable for all obligations subcontracted to, and all acts

and omissions of, the Subprocessor, as foreseen by the Main Agreement and the Regulations.

d. The Controller consents and specifically authorizes the engagement as Subprocessors of the Subprocessors that are listed on the Odoo Privacy Policy as of the date of signature of this Agreement, for the purposes that are described in it.

e. The Customer consents and generally authorizes the engagement as Subprocessors of any other third party provider (such as data center operators, business, engineering and customer support providers), as necessary to support the performance of the Main Agreement, provided that any one of the following situations applies:
   i. the Controller is notified of the engagement of the Subprocessor by the Processor, at least 30 days before the processing takes place, and given the opportunity to object in writing, for reasonable reasons only, within this 30 days period ; or
   ii. the processing by the new Subprocessor is optional and does not take place unless the Controller specifically consents to it ;

f. In case the Controller objects to the engagement of a new Subprocessor under clause “e” and notifies the Processor in writing, the Parties will seek to resolve the matter in good faith. If the Processor is reasonably able to provide the services to the Controller in accordance with the Main Agreement without using the new Subprocessor, and decides in its own discretion to do so, the Controller shall have no further rights under this clause in respect of the engagement of the new Subprocessor. If the Processor requires the use of the new Subprocessor in its own discretion, and is unable to satisfy the Controller as to the suitability and level of protection of the new Subprocessor within 30 days from the Controller’s notification of objection, then the Controller may consider this a breach of the Processor’s obligations under the Main Agreement, and terminate it according to the terms set forth in the Main Agreement.

5. Transfers of personal data to third countries or international organisations

Any transfer of Personal Data outside the European Union (“EU”) or European Economic Area (“EEA”) will be covered by a European Commission adequacy decision or by another appropriate safeguard provided for in the GDPR.

6. Data subjects' right to information

It is the Controller's responsibility to inform the data subjects concerned by the processing operations at the time personal data are being collected, in a concise, transparent, comprehensible and easily accessible manner, in clear and simple terms.

7. Exercise of data subjects' rights

The Processor shall assist the Controller, insofar as this is possible, for the fulfillment of its obligation to respond to requests for exercising the data subject's rights: right of access, to rectification, erasure and to object, right to restriction of processing, right to data portability, right not to be subject to an automated individual decision (including profiling).

Where the data subjects submit requests to the Processor to exercise their rights, the Processor must forward these requests as soon as they are received by email to security@anykey.ch.

8. Notification of personal data breaches

The Processor shall notify the Controller of any personal data breach without undue delay where feasible, under article 33 of GDPR, after having become aware of it and via the following means: security@anykey.ch

Said notification shall be sent along with any necessary documentation to enable the controller, where necessary, to notify this breach to the competent supervisory authority.

9. Controller Assistance

The Processor assists the Controller in carrying out data protection impact assessments.

The Processor undertakes to cooperate with the competent supervisory authority, at the request of the latter or at the request of the Controller, in the performance of the Main Agreement.

In addition, the Processor makes available to the Controller the documentation necessary to demonstrate compliance with its obligations.

10. Security measures

The Processor undertakes to implement necessary security measures to ensure the compliance of the processing with the requirements of the GDPR, including but not limited to the following security measures:

- the encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

11. End of processing

a. The Processor shall, upon expiration or termination of the Agreement and in accordance with the Controller's Instruction, either destroy or return to the

Controller, in a secure way, all personal data (including all copies of the personal data) in its possession or control as soon as reasonably practicable.

b. The personal data from backups could remain stored for up to 12 months, until they are automatically destroyed. The Processor commits not to use those backup copies of the Controller's deleted data for any purpose except for maintaining the integrity of the Controller's backups, unless the Controller or the law require the Processor to do so.

12. The Data Protection Officer

The Processor communicates to the Controller **the name and contact details of its data protection officer**, if it has designated one in accordance with Article 37 of the GDPR, or the equivalent Data Protection Responsible.

13. Record of categories of processing activities

The Processor states that it **maintains a written record** of all categories of processing activities carried out on behalf of the Controller, containing:

- the name and contact details of the Controller on behalf of which the Processor is acting, any other processors and, where applicable, the data protection officer;
- the categories of processing carried out on behalf of the Controller;
- where applicable, transfers of personal data to a third country or an international_organization, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1) of the GDPR, the documentation of suitable safeguards;
- where possible, a general description of the technical and organizational security measures, including but not limited to:
  - the encryption of personal data;
  - the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
  - the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
  - a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

14. Audits

a. The Processor provides the Controller with the **necessary documentation for demonstrating compliance with all of its obligations** and for allowing the Controller or any other auditor it has authorized to reasonably conduct audits, including inspections, and for contributing to such audits.

   i. The Controller may accept as proof of compliance, the provision by the Processor of a valid SOC report and certification, issued by a third party audit firm.

b. The Controller can still send a request for audit to the Data Protection Contact of the Processor and the Parties will discuss and agree in advance on the reasonable start date, duration, scope and security and confidentiality controls applicable to the requested audit. In case the Processor chooses to charge a fee for the audit, it must be based on the Processor's reasonable costs, and the Processor must share the details of the fee and the basis for the calculation in advance. If the Controller chooses to mandate a third-party auditor, the Processor may object to the auditor if it reasonably considers it to be unsuitable, for example if it is a competitor of the Processor. In such a case, the Controller will choose another auditor or conduct the audit themselves.

15. Data Subject Indemnification

a) According to Article 82 of the GDPR, any person who has suffered material or non-material damage as a result of an infringement of the GDPR shall have the right to receive compensation from the Controller or Processor for the damage suffered.
b) Any controller involved in processing shall be liable for the damage caused by processing which infringes the GDPR. The Processor shall be liable for the damage caused by processing only where it has not complied with obligations of the GDPR specifically directed to processors or where it has acted outside or contrary to lawful instructions of the Controller.
c) The Controller or Processor shall be exempt from liability under paragraph b if it proves that it is not in any way responsible for the event giving rise to the damage.
d) Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs b and c, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.
e) Where a controller or processor has, in accordance with paragraph d, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph b.
f) Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79(2).

16. Governing Law

The terms of this Agreement will be governed and construed according to Belgium law. The Parties hereto agree to submit any dispute arising out of or in connection with this DPA to the exclusive jurisdiction of Nivelles, Belgium.

This Agreement is signed in as many copies as there are Parties having a separate interest.

S.B.I.

Done in Volketswil, on 19.02.2024

For the Controller:

Name: Tobias Linder

Position: Chief technology officer

Date: 25.02.2024

Signature:

_____

For the Processor:

Name: Sébastien Bruyr

Position: Chief Commercial Officer

Date: 3/20/2024

Signature:

_____

Appendix I: Description of the processing activities

The Processor is authorized to process, on behalf of and on the instructions of the Controller, the necessary personal data for providing the following service:

a. The nature of operations carried out on the data is:

Database Hosting

The Parties acknowledge that the Controller's database may contain personal data. This data will be processed by the Processor when the Controller instructs so, by using any of the services that require a database (e.g. the Cloud Hosting Services or the Database Upgrade Service), or if the Controller transfers their database or a part of their database to the Processor for any reason pertaining to the Odoo Enterprise Agreement.

Detailed process: storing and processing company data of anykey IT AG

b. The purpose(s) of the processing is:

Supply of specified business applications (license of the Odoo Software), Database Update Service, Infrastructure and Hosting on Cloud environment.

c. The personal data processed are:

contact information, financial information

d. The categories of data subjects are:

Employees
Suppliers
Customers
Job applicants
Consultants
Visitors
Prospects
Trainees

S.B.I.