Data Processing Addendum

Futurae Technologies AG, V1.9.2

This Data Processing Addendum ("**Addendum**") forms part of the master subscription agreement or other similar type agreement pertaining to the Processing of Customer Personal Data (the "**Agreement**") between Futurae Technologies AG ("**Futurae**") and Customer (collectively the "**Parties**"). This Addendum does not replace nor supersede any pre-existing obligations of the Parties; but rather augments such obligations in context of certain applicable laws and regulations pertaining to the handling and processing of Customer Personal Data.

HOW TO EXECUTE THIS DPA:

1. Complete the information required for "Customer Designated POC" on page 5;
2. Sign where indicated on page 6; and
3. Return the signed Addendum to Futurae via dpo@futurae.com

This Addendum shall become legally binding once Futurae receives a validly completed and signed copy from Customer.

This Addendum shall not become legally binding unless Customer has executed a valid Agreement and/or Order Form pursuant to such an Agreement.

1. Subject Matter and Duration

1. **Subject Matter.** This Addendum reflects the Parties' commitment to abide by Applicable Data Protection Laws concerning the Processing of Customer Personal Data in connection with Futurae's execution of the Agreement. All capitalized terms that are not expressly defined in this Data Processing Addendum will have the meanings given to them in the Agreement. If and to the extent language in this Addendum or any of its Exhibits conflicts with the Agreement, this Addendum shall control.
2. **Duration and Survival.** This Addendum will become legally binding upon the Effective Date of the Agreement or upon the date upon which both Parties have signed this Addendum if it is completed after the Effective Date of the Agreement. Futurae will Process Customer Personal Data until the relationship terminates as specified in the Agreement. Futurae's obligations and Customer's rights under this Addendum will continue in effect so long as Futurae Processes Customer Personal Data.

2. Definitions

For the purposes of this Addendum, the following terms and those defined within the body of this Addendum apply.

1. "**Applicable Data Protection Law(s)**" means the relevant data protection and data privacy laws, rules, and regulations to which the Customer Personal Data are subject. "Applicable Data Protections Law(s)" shall include, but not be limited to, EU General Data Protection Regulation 2016/679 ("GDPR") principles and requirements.
2. "**Customer Personal Data**" means Personal Data pertaining to Customer's users or employees (data subjects under EU GDPR) located in the European Economic Area Processed by Futurae. The Customer Personal Data and the specific processing of the Customer Personal Data are detailed in **Exhibit A** attached hereto, as required by the GDPR.
3. "**Controller**" means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
4. "**Personal Data**" shall have the meaning assigned to the terms "personal data" or "personal information" under Applicable Data Protection Law(s).
5. "**Process**," "**Processes**," "**Processing**," "**Processed**" means any operation or set of operations which is performed on data or sets of data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.
6. "**Processor**" means a natural or legal person, public authority, agency, or other body which Processes Customer Personal Data on behalf of Customer subject to this Addendum.

7. “**Security Incident(s)**” means the breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data Processed by Futurae.

8. “**Services**” means any and all services that Futurae performs under the Agreement.

9. “**Third Party(ies)**” means Futurae’s authorized contractors, agents, vendors and third party service providers that Process Customer Personal Data (i.e., subprocessors).

3. Data Use and Processing

1. Compliance with Laws. Customer Personal Data shall be Processed in compliance with the terms of this Addendum and all Applicable Data Protection Law(s).

2. Documented Instructions. Futurae and its Third Parties shall Process Customer Personal Data only in accordance with the documented instructions of Customer or as specifically authorized by this Addendum, the Agreement, or any applicable Statement of Work. Futurae will, unless legally prohibited from doing so, inform Customer in writing if it reasonably believes that there is a conflict between Customer’s instructions and applicable law or otherwise seeks to Process Customer Personal Data in a manner that is inconsistent with Customer’s instructions.

3. Authorization to Use Third Parties. To the extent necessary to fulfill Futurae’s contractual obligations under the Agreement or any Statement of Work, Customer hereby authorizes Futurae to engage Third Parties (including subprocessors). Any Third Party Processing of Customer Personal Data shall be consistent with Customer’s documented instructions and comply with all Applicable Data Protection Law(s).

4. Futurae and Third Party Compliance. Futurae agrees to (i) enter into a written agreement with Third Parties regarding such Third Parties’ Processing of Customer Personal Data that imposes on such Third Parties (including subprocessors) data protection and security requirements for Customer Personal Data that are compliant with Applicable Data Protection Law(s); and (ii) remain responsible to Customer for Futurae’s Third Parties’ failure to perform their obligations with respect to the Processing of Customer Personal Data.

5. Right to Object to Third Parties. Futurae shall make available to Customer a list of Third Parties that Process Customer Personal Data through its website at https://www.futurae.com/legal/subprocessors/. Prior to engaging any new Third Parties that Process Customer Personal Data, Futurae will notify Customer via email and allow Customer thirty (30) days to object. If Customer has legitimate objections to the appointment of any new Third Party, the parties will work together in good faith to resolve the grounds for the objection for no less than thirty (30) days, Futurae disclosing parts of the relevant data protection agreements in its reasonable discretion, and failing any such resolution, Customer may terminate the part of the service performed under the Agreement that cannot be performed by Futurae without use of the objectionable Third Party. Futurae shall refund any pre-paid fees to Customer in respect of the terminated part of the Service.

6. Confidentiality. Any person or Third Party authorized to Process Customer Personal Data must agree to maintain the confidentiality of such information or be under an appropriate statutory or contractual obligation of confidentiality.

7. Personal Data Inquiries and Requests. Futurae agrees to comply with all reasonable instructions from Customer related to any requests from individuals exercising their rights related to Personal Data granted to them under Applicable Data Protection Law(s) (“**Privacy Request**”). At Customer’s request and without undue delay, Futurae agrees to assist Customer in answering or complying with any Privacy Request in so far as it is possible.

8. Data Protection Impact Assessment and Prior Consultation. Futurae agrees to provide reasonable assistance at Customer’s expense to Customer where, in Customer’s judgement, the type of Processing performed by Futurae is likely to result in a high risk to the rights and freedoms of natural persons (e.g., systematic and extensive profiling, Processing sensitive Personal Data on a large scale and systematic monitoring on a large scale, or where the Processing uses new technologies) and thus requires a data protection impact assessment and/or prior consultation with the relevant data protection authorities.

9. Demonstrable Compliance. Futurae agrees to keep records of its Processing in compliance with Applicable Data Protection Law(s) and provide any necessary records to Customer to demonstrate compliance upon reasonable request.

4. Cross-Border Transfers of Personal Data

1. A “**Restricted Transfer**” is a transfer of Personal Data from one of the parties to this Addendum to the extent that such transfer would be prohibited under the applicable Data Protection Laws without agreement to the Standard Contractual Clauses.

2. Customer (as data exporter) and Futurae (as data importer) hereby agree, and for each Restricted Transfer from Customer to Futurae, the general clauses and respectively Module 2 of the "Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, currently available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN#d1e32-61-1 (“Standard Contractual Clauses” or “SCC”) shall automatically apply. In connection therewith, the following will apply: (i) the signing of this DPA will also be deemed signing of the SCC (Annex I.A.), (ii) Exhibit A of this DPA also as Annex I.B. of the Standard Contractual Clauses and (iii) Section 5 of this DPA also as Annex II of the Standard Contractual Clauses. Further, the following will apply: Clause 9(a) is included as option 2, subject to a minimum of two weeks' notice from the data importer prior to the engagement of the sub-processor; Clause 11(a) is included without option.

3. In the case of Restricted Transfers from Switzerland, references by the SCC to member states are also to be understood as references to Switzerland and the Federal Data Protection and Information Commissioner (FDPIC) is the competent authority in accordance with Clause 13 of the SCC. This also applies in the case of onward transmission of personal data transmitted from Switzerland. If a Restricted Transfer is subject to the GDPR, the authority named in Annex 1 is responsible (possibly parallel to the FDPIC).

4. The applicable law and competent court under Clauses 17 and 18 of the SCC are governed by the Agreement, unless the Restricted Transfer is subject to the GDPR; in this respect, Liechtenstein law applies and the courts of Vaduz are responsible.

5. Insofar as a new version of the standard contractual clauses is adopted as binding, this new version shall be deemed to have been agreed upon at the time it comes into force.

6. Futurae undertakes not to carry out any Restricted Transfers without suitable guarantees within the meaning of the Applicable Data Protection Law(s) (e.g. SCC with the corresponding modules with the recipient concerned).

5. Information Security Program

1. Futurae agrees to implement appropriate technical and organizational measures designed to protect Customer Personal Data as required by Applicable Data Protection Law(s) and as may be further described in the Agreement (the “**Information Security Program**”). Such measures shall include:

   - Pseudonymization of Customer Personal Data where appropriate, and encryption of Customer Personal Data in transit;
   - Technical and organizational security measures in accordance with the recognized market standards in order to protect personal data stored with us against unintentional, illegal or unauthorized manipulation, deletion, modification, access, disclosure, or use, as well as against partial or complete loss;
   - The Futurae websites and server infrastructure, responsible for providing Futura’s online services are located at secure, certified data centers in Switzerland and in the United Kingdom;
   - When personal data is transmitted over the network, it is protected through the use of state-of-the-art encryption, such as the Transport Layer Security (TLS) protocol;
   - Customer data is backed up on a regular basis;
   - Security measures are continuously adapted and improved in line with technological developments.
   - Regular training of Futurae employees to ensure compliance with data security practices;
   - Implementation of complex passwords and regular password updates to reduce the risk of hacking;
   - Regular reviews to consider data minimization measures is maintained at an optimal level;
   - A process for regularly testing, assessing and evaluating of the effectiveness of Futurae’s Information Security Program to ensure the security of Customer Personal Data from reasonably suspected or actual accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access.

6. Security Incidents

1. Security Incident Procedure. Futurae will deploy and follow policies and procedures to detect, respond to, and otherwise address Security Incidents including procedures to (i) identify and respond to reasonably suspected or known Security Incidents, mitigate harmful effects of Security Incidents, document Security

Incidents and their outcomes, and (ii) restore the availability or access to Customer Personal Data in a timely manner.

2. Notice. Futurae agrees to provide prompt written notice without undue delay and within the time frame required under Applicable Data Protection Law(s) (but in no event longer than forty-eight (48) hours) to Customer's Designated POC if it knows or reasonably suspects that a Security Incident has taken place. Such notice will include all available details required under Applicable Data Protection Law(s) for Customer to comply with its own notification obligations to regulatory authorities or individuals affected by the Security Incident.

7. Audits

1. Right to Audit; Permitted Audits. Futurae shall make available to Customer and its regulators all information necessary to demonstrate compliance with Applicable Data Protection Laws and this Addendum. Customer and its regulators shall have the right to inspect Futurae's architecture, systems, and documentation which are relevant to the security and integrity of Customer Personal Data, or as otherwise required by a governmental regulator:
   - Following any notice from Futurae to Customer of an actual or reasonably suspected Security Incident involving Customer Personal Data;
   - Upon Customer's reasonable belief that Futurae is not in compliance with Applicable Data Protection Laws, this Addendum or its security policies and procedures under the Agreement;
   - As required by governmental regulators;
   - Or otherwise in accordance with GDPR regulations.
2. Audit Terms. Any audits described in this Section shall be:
   - Conducted by Customer or its regulator, or through a third party independent contractor selected by one of these parties.
   - Conducted during reasonable times.
   - Conducted upon reasonable advance notice to Futurae.
   - Of reasonable duration and shall not unreasonably interfere with Futurae's nor Third Party day-to-day operations.
   - Conducted in such a manner that does not violate any agreement between Futurae and its cloud providers.
3. Third Parties. In the event that Customer conducts an audit through a third party independent auditor or a third party accompanies Customer or participates in such audit, such third party shall be required to enter into a non-disclosure agreement containing confidentiality provisions substantially similar to those set forth in the Agreement to protect Futurae's and Futurae's customers' confidential and proprietary information. For the avoidance of doubt, regulators shall not be required to enter into a non-disclosure agreement.
4. Audit Results. Upon Futurae's request, after conducting an audit, Customer shall notify Futurae of the manner in which Futurae does not comply with any of the applicable security, confidentiality or privacy obligations or Applicable Data Protection Laws herein. Upon such notice, Futurae shall make any necessary changes to ensure compliance with such obligations at its own expense and without unreasonable delay and shall notify Customer when such changes are complete. Notwithstanding anything to the contrary in the Agreement, Customer may conduct a follow-up audit within six (6) months of Futurae's notice of completion of any necessary changes. To the extent that a Futurae audit and/or Customer audit identifies any material security vulnerabilities, Futurae shall remediate those vulnerabilities within fifteen (15) days of the completion of the applicable audit, unless any vulnerability by its nature cannot be remedied within such time, in which case the remediation must be completed within a mutually agreed upon time not to exceed sixty (60) days.

8. Data Storage and Deletion

1. Data Storage. Futurae will abide by the following with respect to storage of Customer Personal Data:
   - Futurae will not store or retain any Customer Personal Data except as necessary to perform the Services under the Agreement.
   - Futurae uses subprocessors' cloud services which process and store Personal Data in one or more countries. Customer may contact Futurae for any queries regarding countries where Customer Personal Data is Processed or stored.
2. Data Deletion. Futurae will abide by the following with respect to deletion of Customer Personal Data:

- Within thirty (30) calendar days of the Agreement's expiration or termination, or sooner if requested by Customer, Futurae will securely destroy all copies of Customer Personal Data.
- Upon Customer's request, Futurae will promptly return to Customer a copy of all Customer Personal Data within thirty (30) days and, if Customer also requests deletion of the Customer Personal Data, will carry that out as set forth above.
- Deletion of Customer Personal Data will be conducted in accordance with standard industry practices.
- Upon Customer's request, Futurae will provide evidence that Futurae has deleted all Customer Personal Data. Futurae will provide the "Certificate of Deletion" within thirty (30) days of Customer's request.

9. Contact Information

1. Futurae and the Customer agree to designate a point of contact for urgent privacy and security issues (a "**Designated POC**"). The Designated POC for both parties are:
   - Futurae Designated POC: dpo@futurae.com
   - Customer Designated POC: ___________________________

Signature

On behalf of Customer

Signature:

Print Name:

Title:

Date:

Signature (if required):

Print Name:

Title:

Date:

On behalf of Futurae Technologies AG

Signature:

Print Name:

Title:

Date:

Signature (if required):

Print Name:

Title:

Date:

Exhibit A

1. Subject Matter of Processing

The subject matter of Processing is the Services pursuant to the Agreement and the subject matter of any sub-processing shall also be pursuant to the Agreement, together with the terms of any sub-contract.

2. Duration of Processing

The Processing (and any sub-processing) will continue until the expiration or termination of the Agreement (or in the case of sub-processors, any sub-contract).

3. Categories of Data Subjects

Includes the following:

- Prospects, customers, business partners and vendors of Customer (who are natural persons)

4. Nature and Purpose of Processing

Includes the following:

- Nature: Processing in Futurae's Authentication as a Service applications (to the extent purchased by Customer) of the data uploaded by Customer or collected by Futurae via its applications, APIs and SDKs.
- The purpose of Processing of Customer Personal Data by Futurae is the performance of the Services pursuant to the Agreement.

5. Types of Personal Information

- In relation to Customer's customers, includes the following: Usernames, randomly generated identifiers and cryptographic keys.
- When using Futurae's adaptive authentication technologies (pseudonymized, and following explicit permission granting by the Customer's customer):
  - Geolocation information (GPS-based, GeoIP location)
  - WiFi networks scan
  - Bluetooth devices scan
  - Connected WiFi network
  - Connected Bluetooth devices
  - Connected devices in the same network
  - Nearby devices
- Traffic data, as well as information about device hardware and software. This information includes: IP address, browser/OS/mobile device information, domain names, access times, browser fingerprint, cookie, gyroscope, accelerometer, and referring website addresses.
- Data related to the use of the Customers' services, such as transaction history or communication events.

In relation to Customer, includes the following:

- Basic personal data (such as name) and contact details (such as email, phone number etc).
- Data related to content of communication, such as e-mails, voice mails, SMS, browsing data etc.