Data Processing Addendum

Futurae Technologies AG ("**Futurae**") and the counterparty agreeing to these terms ("**Customer**") (collectively the "**Parties**") have entered into an agreement in respect of the Services pursuant and subject to either (i) Futurae's standard terms of service or (ii) where the Parties have executed a master subscription agreement or any other written agreement, those terms ("**Main Agreement**"). This Data Processing Addendum, including any annexes ("**DPA**") forms part of the Main Agreement.

Effective as of the date on which Customer signed, or the Parties otherwise agreed to, this DPA ("**DPA Effective Date**"), this DPA shall replace and supersede any previously applicable terms and conditions pertaining to their subject matter incorporated into the Main Agreement (including any data processing amendment, agreement or addendum relating to the Services). For clarity, this DPA shall be of no use and effect if signed by anyone which is not a Customer.

Capitalized terms not expressly defined in this DPA will have the meaning given to them in the Main Agreement.

HOW TO EXECUTE THIS DPA:

- Complete the Customer contact details for notices under clause 8 of this DPA;
- Insert your signature in the field indicated in this DPA; and
- Return a copy of the signed DPA to Futurae by email to dpo@futurae.com.

1. Personal Data processing

1.1. The following definitions apply in this DPA:

"**Adequate Country**" means country or territory that is recognized under European Law as providing adequate protection for Personal Data.

"**Applicable Data Protection Law**" means the law and regulation applicable to processing of Personal Data under the Main Agreement in any part of the world where Futurae provides the Services, including but not limited to European Law and US Law.

"**Customer Personal Data**" means Personal Data pertaining to Customer's users or employees (data subjects under the EU GDPR or the UK GDPR) located in the EEA and processed by Futurae. The Customer Personal Data and the specific processing of the Customer Personal Data are detailed in Exhibit 1 attached hereto.

"**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.

"**European Law**" means the law and regulation of the European Union ("**EU**"), the European Economic Area ("**EEA**"), their member states, Switzerland, and the United Kingdom applicable to the processing of Personal Data under the Main Agreement (including, as applicable, (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) ("**EU GDPR**"); (ii) the EU GDPR as retained into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 and the UK Data Protection Act 2018 ("**UK GDPR**"); (iii) the Swiss Federal Data Protection Act of 25 September 2020 and its corresponding ordinances ("**Swiss DPA**"); (iv) the EU e-Privacy Directive (Directive 2002/58/EC); and (v) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii), (iii), (iv) and any amending, updating or replacing legislation or regulation from time to time in force.

"**EU SCCs**" means the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to the EU GDPR.

"**Personal Data**" shall have the meaning assigned to the terms "personal data" or "personal information" or "personally identifiable information" or similar terms under Applicable Data Protection Law.

"**processing**", "**data subject**" and "**supervisory authority**" shall have the meaning ascribed to them in European Law.

"**Processor**" means a natural or legal person, public authority, agency, or other body which processes Personal Data on behalf of the Controller, including an entity to which another entity discloses a natural individual's personal information for a business purpose pursuant to a written contract that requires the entity receiving the information to only retain, use, or disclose Personal Data for the purpose of providing the Services, and includes "processor", "service provider" or any otherwise analogous term defined under the Applicable Data Protection Law.

"**Restricted Transfer**" means: (i) where the EU GDPR or Swiss DPA applies, a transfer of Personal Data from the EEA or Switzerland (as applicable) to a country outside of the EEA or Switzerland (as applicable) which is not subject to an adequacy determination by the European Commission or Swiss Federal Data Protection and Information Commissioner (as applicable); and (ii) where the UK GDPR applies, a transfer of Personal Data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018.

"**Personal Data Breach**" means the breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed for the purpose of providing the Services to Customer by Futurae its sub-Processors, or any other identified or unidentified third party.

"**Services**" means any and all services that Futurae performs under the Main Agreement.

"**UK Addendum**" means the International Data Transfer Addendum (Version B1.0) issued by the Information Commissioner's Office under s.119(A) of the UK Data Protection Act 2018, as updated or amended from time to time.

"**US Law**" means the law and regulation of the United States applicable to the processing of Personal Data under the Main Agreement, including (i) the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (Cal. Civ. Code § 1798.100 - 1798.199, 2022) and its implementing regulations ("**CCPA**"), (ii) the Virginia Consumer Data Protection Act, when effective, (iii) the Colorado Privacy Act and its implementing regulations, when effective, (iv) the Utah Consumer Privacy Act, when effective; and (v) Connecticut SB6, An Act Concerning Personal Data Privacy and Online Monitoring, when effective, (vi) the applicable data protection laws made at federal or state level from time to time in force; and any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii), (iii), (iv), (vi) and any amending, updating or replacing legislation or regulation from time to time in force.

1.2. Any reference in this DPA to "providing" the Services means delivering the Services as defined in the Main Agreement;

2. Relationship of the parties

2.1. The type of Personal Data processed pursuant to this DPA and the subject matter, duration, nature and purpose of the processing, and the categories of data subjects, are as described in Annex 1.

2.2. In respect of the parties' rights and obligations under this DPA regarding the Personal Data:

2.2.1. each Party warrants in relation to Personal Data that it will comply with and provide the same level of privacy protection as required by the Applicable Data Protection Law;

2.2.2. as between the Parties, the Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which the Customer acquired Personal Data;

2.2.3. the Parties acknowledge and agree that the Customer is the Controller (or a Processor processing Personal Data on behalf of a third-party Controller), and Futurae is a Processor (or sub-Processor, as applicable).

2.3. Customer warrants to Futurae, where Customer is a Processor, that Customer's instructions and actions with respect to the Personal Data, including its appointment of Futurae as another Processor and, where applicable, concluding the EU SCCs (including as they may be amended as described in this DPA), have been (and will, for the duration of this DPA, continue to be) authorized by the relevant third-party Controller.

3. Personal Data processing

3.1. Where it processes Personal Data as a Processor (or sub-Processor), Futurae warrants that it will:

3.1.1. only process Personal Data for the limited and specified business purpose of providing the Services and in accordance with:

(i) the requirements of Applicable Data Protection Law;

(ii) the Customer's written instructions as set out in this DPA, the Main Agreement, or any applicable Order, Statement of Work or other document entered into pursuant and subject to the Main Agreement, unless prohibited from doing so under applicable law or regulation.

3.1.2. not use Personal Data for the purposes of marketing or advertising;

3.1.3. implement appropriate technical and organizational measures to ensure a level of security which is appropriate to the risks that are presented by the processing of Personal Data, in particular protection against the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data. Such measures include, without limitation, the security measures set out in Annex 2 ("**Security Measures**"). Customer acknowledges that the Security Measures remain at all times subject to technical advancements and development and that Futurae may update or amend the Security Measures from time to time at its sole discretion, provided that such updates and modifications do not degrade or diminish the overall security of the Service;

3.1.4. ensure that solely authorized personnel have access to Personal Data and, where authorized, must agree to maintain the confidentiality of such information or be under an appropriate statutory or contractual obligation of confidentiality;

3.1.5. comply with all reasonable instructions from Customer related to any requests from a data subject exercising their rights related to Personal Data granted to them under Applicable Data Protection Law (including rights of access, rectification or erasure) in respect of that data subject's Personal Data ("**Data Subject Request**"). At Customer's request and without undue delay, if Customer does not have the ability to address a Data Subject Request without its input, Futurae agrees to assist Customer in answering or complying with any Data Subject Request in so far as it is possible, subject to Customer:

(i) retaining responsibility for verifying that the requestor is the data subject in respect of whose Personal Data the relevant Data Subject Request was made; and

(ii) agreeing that Futurae shall bear no responsibility for information provided in good faith to Customer in reliance on sub-clause (i) immediately above.

Customer acknowledges and agrees that Futurae will not respond to a Data Subject Request without the Customer's prior written consent, except to confirm that such request relates to the Customer.

3.1.6. taking into account the nature of processing and the information available to it, provide to Customer such assistance as the Customer, acting reasonably, requests in relation to Futurae's obligations under Applicable Data Protection Law and this DPA, in respect of:

(i) data protection impact assessments and prior consultations (as such terms are defined in Applicable Data Protection Law);

(ii) notifications to the supervisory authority under Applicable Data Protection Law and/or communications to data subjects by Customer in response to any Personal Data Breach; and

(iii) Customer's ongoing compliance with its obligations under Applicable Data Protection Law concerning security of processing.

3.1.7. where processing Personal Data on behalf of the Customer within the scope of the CCPA, not retain, use, or disclose that Personal Data for any purposes other than the purposes set out in the Main Agreement and this DPA and as permitted under the CCPA, including under any "sale" exemption. Futurae will not "sell" or "share" such Personal Data, as those terms are defined in the CCPA. This clause 3.1.7 does not, in any way, limit or reduce any data protection commitments Futurae makes to the Customer in the Main Agreement or this DPA.

3.2. Futurae hereby certifies that it shall comply with the obligations and restrictions in clauses 2 and 3, and the Applicable Data Protection Law.

4. Sub-processing

4.1. Futurae undertakes to share Personal Data to sub-Processors solely for the specific purpose of providing the Services. Futurae will ensure that any sub-Processor engaged to provide part of the Service on its behalf in connection with this DPA does so solely on the basis of a written contract which imposes on such sub-Processor data protection obligations terms that are no less protective of Personal Data than those imposed on Futurae under this DPA ("**Relevant Terms**"). Futurae shall procure the performance by such sub-Processor of the Relevant Terms and shall be liable to the Customer for any breach by such sub-Processor of any of the Relevant Terms.

4.2. The Customer grants a general written authorization to Futurae to appoint third party cloud services operators, and business, engineering and customer support providers as sub-Processors to support the performance of the Service.

4.3. Futurae maintains a list of sub-Processors at https://www.futurae.com/legal/subprocessors/ and will update it with the names of new and replacement sub-Processors at least thirty (30) days prior to the date on which those sub-Processors commence processing of Personal Data. If Customer objects to any new or replacement sub-Processor on reasonable grounds related to data protection, it shall notify Futurae of such objections in writing within ten (10) days of the notification and the parties will seek to resolve the matter in good faith. If Futurae is reasonably able to provide the affected Services to the Customer in accordance with the Main Agreement without using the sub-Processor and decides in its discretion to do so, the Customer will have no further rights under this clause 4.3 in respect of the proposed use of the sub-Processor. If Futurae, in its discretion, requires use of the sub-Processor and is unable to satisfy Customer's objection regarding the proposed use of the new or replacement sub-Processor, then Customer may terminate the applicable Order Form effective upon the date Futurae begins use of such new or replacement sub-Processor solely with respect to those Services that will use the proposed new sub-Processor for the processing of Personal Data. If Customer does not provide a timely objection to any new or replacement sub-Processor in accordance with this clause 4.3, Customer will be deemed to have consented to the sub-Processor and waived its right to object.

5. Personal Data Transfers from the EEA, Switzerland and the UK

5.1. In connection with the Services, the parties acknowledge that Futurae (and its sub-Processors) may process outside of Switzerland, the EEA and the United Kingdom, certain Personal Data protected by European Law for which Customer may be a Controller (or Processor on behalf of a third-party Controller, as the case may be) unless Customer subscribes to a service that restricts data processing to a specific Adequate Country.

5.2. Both parties agree that when the transfer of Personal Data protected by European Law from Customer to Futurae is a Restricted Transfer then it shall be subject to the appropriate protections as follows:

5.2.1. **EEA Transfers**: in relation to Personal Data protected by the EU GDPR, the EU SCCs will apply completed as follows:

(i) Module Two will apply where Customer is a Controller and Module Three will apply where Customer is a Processor;

(ii) in Clause 7, the optional docking clause will apply;

(iii) in Clause 9, Option 2 will apply, and the time period for prior notice of sub-Processor changes shall be as set out in Clause 4.3 of this DPA;

(iv) in Clause 11, the optional language will not apply;

(v) in Clause 17, Option 2 will apply, and if the data exporter's Member State does not allow for third-party beneficiary rights, then the law of Switzerland shall apply;

(vi) in Clause 18(b), disputes shall be resolved before the courts of the jurisdiction governing the Main Agreement between the parties or, if that jurisdiction is not an EU Member State, then the courts in Zurich, Switzerland shall be the designated forum. In any event, Clause 17 and 18 (b) shall be consistent in that the choice of forum and jurisdiction shall fall on the country of the governing law;

(vii) Annex I of the EU SCCs shall be deemed completed with the information set out in Annex 1 to this DPA; and

(viii) Annex II of the EU SCCs shall be deemed completed with the information set out in Annex 2 to this DPA.

5.2.2. **Swiss Transfers**: in relation to Personal Data protected by the Swiss DPA, the EU SCCs, completed as set out above in clause 5.2.1 of this DPA, shall apply to transfers of such Personal Data, except that:

(i) the supervisory authority in respect of Personal Data shall be the Swiss Federal Data Protection and Information Commissioner;

(ii) references to "Member State(s)" in the EU SCCs shall be interpreted to refer to Switzerland, and data subjects located in Switzerland shall be entitled to exercise and enforce their rights under the EU SCCs in Switzerland; and

(iii) references to the "General Data Protection Regulation", "Regulation 2016/679" or "GDPR" in the EU SCCs shall be understood to be references to the Swiss DPA.

5.2.3. **UK Transfers**: in relation to Personal Data that is protected by the UK GDPR, the EU SCCs, completed as set out above in clause 5.2.1 of this DPA, shall apply to transfers of such Personal Data, except that:

(i) the EU SCCs shall be deemed amended as specified by the UK Addendum, which shall be deemed executed between the transferring Customer (or the relevant member of the Customer Group) and Futurae;

(ii) any conflict between the terms of the EU SCCs and the UK Addendum shall be resolved in accordance with Section 10 and Section 11 of the UK Addendum;

(iii) for the purposes of the UK Addendum, Tables 1 to 3 in Part 1 of the UK Addendum shall be deemed completed using the information contained in the Annexes of this DPA; and

(iv) Table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "neither party".

5.2.4. The following terms shall apply to the EU SCCs (including as they may be amended under clauses 5.2.2 and 5.2.3 above):

(i) Customer may exercise its right of audit under the EU SCCs as set out in, and subject to the requirements of, clause 7 of this DPA; and

(ii) Futurae may appoint sub-Processors as set out in, and subject to the requirements of, clauses 4 and 5.3 of this DPA, and Customer may exercise its right to object to sub-Processors under the EU SCCs in the manner set out in clause 4.3 of this DPA.

5.2.5. Should any provision of this DPA contradict, directly or indirectly, the EU SCCs (and the UK Addendum, as appropriate), the latter shall prevail.

5.3. In respect of Restricted Transfers made to it under clause 5.2, Futurae shall not participate in (nor permit any sub-Processor to participate in) any further Restricted Transfers of Personal Data (whether as an "exporter" or an "importer" of the Personal Data) unless such further Restricted Transfer is made in full compliance with European Law and pursuant to EU SCCs implemented between the exporter and importer of the Personal Data or an Alternative Transfer Mechanism (as defined in clause 5.5) adopted by the importer applies.

5.4. In the event Customer seeks to conduct any assessment of the adequacy of the EU SCCs for transfers to any particular countries or regions, Futurae shall, to the extent it is able, provide reasonable assistance to Customer for the purpose of any such assessment, provided that Customer covers all costs incurred by Futurae in doing so.

5.5. Should Futurae at any time adopt an alternative data export mechanism (including any new version of or successor to the Privacy Shield adopted pursuant to applicable European Law) for the transfer of Personal Data not described in this DPA ("**Alternative Transfer Mechanism**"), the Alternative Transfer Mechanism shall apply instead of any applicable transfer mechanism described in this DPA (but only to

the extent such Alternative Transfer Mechanism complies with European Law and extends to the territories to which Personal Data is transferred), and Customer agrees to execute such other and further documents and take such other and further actions as may be reasonably necessary to give legal effect to such Alternative Transfer Mechanism.

6. Personal Data Breach

6.1. Futurae will deploy and follow policies and procedures to detect, respond to, and otherwise address any Personal Data Breach, including procedures to:

6.1.1. identify and respond to those reasonably suspected or known, mitigate their harmful effects, document them and their outcomes; and

6.1.2. restore the availability or access to Customer Personal Data in a timely manner.

6.2. Without undue delay, Futurae will notify the Customer on becoming aware that a Personal Data Breach has taken place. Such notice will include all available details in Futurae's possession concerning such Personal Data Breach insofar as it affects the Personal Data, as required under Applicable Data Protection Law and Futurae shall provide reasonable cooperation and assistance to Customer in respect of that Personal Data Breach.

6.3. Futurae will not make any public announcement about a Personal Data Breach without the prior written consent of the Customer, unless required under applicable law.

7. Audit

7.1. Futurae shall, in accordance with Applicable Data Protection Law, make available to Customer (and for the purposes of this clause 7 any reference to Customer shall be deemed to include its supervisory authority) all information in Futurae's possession and control reasonably requested to demonstrate compliance with its obligations as Processor under Applicable Data Protection Law and this DPA in respect of its processing of Personal Data.

7.2. Futurae may fulfil a Customer's right of audit under Applicable Data Protection Law in relation to Personal Data, by providing, in response to a request by Customer sent to compliance@futurae.com, either:

7.2.1. an audit report not older than one year, prepared by an independent external auditor demonstrating that Futurae's technical and organizational measures are sufficient and in line with accepted industry audit standard;

7.2.2. additional information in Futurae's possession or control when additional information is required in relation to the processing of Personal Data carried out by Futurae under this DPA; and

7.2.3. if Customer's Personal Data is subject to the either EU SCCs or the UK Addendum and the information made available pursuant to this clause 7 is insufficient to Customer, acting reasonably, to confirm Futurae's compliance with its obligations under Applicable Data Protection Law or this DPA, then Futurae shall enable Customer to request one onsite audit per annum during the term of the Main Agreement, subject to clause 7.3 below.

7.3. Customer shall follow the procedure below when requesting an audit under clause 7.2.3 above:

7.3.1. Futurae and Customer will discuss and agree in advance on the reasonable start date, scope, duration of, and security and confidentiality controls applicable to any audit under clause 7.2.3. Whenever possible, evidence for such an audit will be limited to the evidence collected for Futurae's most recent third-party audit.

7.3.2. Any reasonable costs incurred by Futurae may be charged to the Customer as a fee for any audit request under clause 7.2.3, with Futurae providing the Customer with further details of any applicable fee, and its cost basis, in advance of any such audit. Customer will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit.

7.3.3. Futurae may object in writing to an auditor appointed by Customer to conduct any audit under clause 7.2.3 if the auditor is, in Futurae's opinion, acting reasonably, not suitably qualified or independent, a competitor of Futurae, or otherwise manifestly unsuitable (i.e., an auditor whose engagement may have a harmful or undesired impact on Futurae's business). Futurae's objection will require the Customer to appoint another auditor or conduct the audit itself. If the EU SCCs

or UK Addendum (including as they may be amended in clauses 5.2.2 and 5.2.3 above) applies, nothing in this clause 7.3 varies or modifies the EU SCCs or the UK Addendum nor affects any supervisory authority's or data subject's rights therein.

8. Notices

8.1. The Parties' contact details for notices under this DPA are:

- for Futurae: dpo@futurae.com
- for Customer: _____

Signature Page

On behalf of Customer

Signature	Signature (if required)
Print Name	Print Name
Title	Title
Date	Date

On behalf of Futurae Technologies AG

Signature	Signature
 **Nikolaos Karapanos, CISO & co-founder** Zurich, 9 May 2025 AES **Advanced electronic signature** Signed on Skribble.com	 9 May 2025 AES **Advanced electronic signature** Signed on Skribble.com
Print Name NIKOLAOS KARAPANOS	Print Name SANDRA TOBLER
Title CTO	Title CCO

Annex 1

This Annex 1 forms part of the DPA and describes the processing performed by Futurae on behalf of Customer.

A. LIST OF PARTIES

Data exporter(s):

Question	**Answer**
Name of Customer and any Customer Affiliates	As stated in the Main Agreement
Address of Customer and any Customer Affiliates	As stated in the Main Agreement
Contact person's name, role and contact details	As stated in the Main Agreement
Activities relevant to the personal data transferred under this DPA (and EU SCCs or IDTA, where applicable)	Use of the Services pursuant to the Main Agreement
Deemed execution date for Annex 1	Upon execution of the DPA
Role (controller / processor)	Controller (or processor on behalf of third-party controller)

Data importer(s):

Question	**Answer**
Name	Futurae Technologies AG
Address	Eichstrasse 23, 8045 Zürich, Switzerland
Contact person's name, role and contact details	Nikos Karapanos Data Protection Officer dpo@futurae.com
Activities to the personal data transferred under this DPA (and EU SCCs or IDTA, where applicable)	Processing which is necessary to provide the Services to Customer pursuant to the Main Agreement
Deemed execution date for Annex 1	Upon execution of the DPA
Role (controller / processor)	Processor (sub-processor)

Data Processing and Transfer of Personal Data:

Question	**Answer**
Categories of data subjects whose Personal Data is being transferred	Natural persons which (i) access or use Customer's services or (ii) are Customer's personnel, partners, vendors or agents, in each case accessing or using Futurae's Services (End Users).
Categories of Personal Data transferred	Profile or Contact Data: Futurae processes this information (for example, Name, Email, Phone number, Account password) directly from End Users, when they choose to give it to us expressly (such as when signing up for an account) or when Customer determines in its sole discretion to make it available to Futurae as part of the Services (for example, Username, Randomly Generated Identifier, Cryptographic Key) to enable Futurae to provide the Services and perform the contract.

	Device Data: Futurae processes this information (for example, Type of device used to access the Services, Operating system), pseudonymised from End Users when they choose to give it to Futurae expressly as part of the Services or automatically when End Users choose to use certain Services such as Futurae Adaptive (for example, Geolocation, WiFi networks scan, Bluetooth devices scan, Connected WiFi network, Connected Bluetooth devices, Connected devices in the same network, Device sensors, Nearby devices), in each case to enable Futurae to provide the Services and perform the contract. Internet Traffic Data: Futurae processes this information (for example, Network traffic data such as IP address, Browser and browser fingerprint, Domain, Time stamp, Cookie or Referring web address) automatically when End Users choose to give it to Futurae expressly as part of the Services, to enable Futurae to provide the Services and perform the contract. Usage Data: Futurae processes this information (for example, How often various Service features are used, Inferences drawn from Service usage data) automatically when End Users use the Futurae Services, to understand feature usage and improve our Services.
Sensitive data transferred (if applicable) and having applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures	No sensitive data. Any such special categories of data shall be protected by applying the security measures described in Annex 2.
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)	Continuous for the duration of the Main Agreement.
Nature of the processing	Processing necessary to provide the Futurae Services to Customer in accordance with the documented instructions provided in the Main Agreement and this DPA.
Purpose(s) of the data transfer and further processing	Processing necessary to provide the Futurae Services to Customer in accordance with the documented instructions provided in the Main Agreement and this DPA.
The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period	Until (i) expiry/termination of the Main Agreement, or (ii) the date upon which processing is no longer necessary for the purposes of either party performing its obligations under the Main

	Agreement (to the extent applicable, whichever is latest).
For transfers to (sub-) Processors, also specify subject matter, nature and duration of the processing	The subject matter, nature and duration of the processing shall be as specified in the Main Agreement.

Competent Supervisory Authority:

Question	**Answer**
Identify the competent supervisory authorities (e.g. in accordance with Clause 13 of the EU SCCs)	In respect of the EU SCCs, means the competent supervisory authority determined in accordance with Clause 13 of the EU SCCs. In respect of the UK Addendum, means the UK Information Commissioner's Office.

Annex 2 - Technical and Organisational Security Measures

Futurae has implemented and shall maintain an information security program in accordance with the ISO/IEC 27001 standard to which it is subject. Futurae's security program shall include the following measures and processes:

1. Encryption of Personal Data

1.1. Futurae has implemented encryption to adequately and effectively protect Personal Data using:

1.1.1. best-in-class encryption protocols designed to provide protection against active or passive attacks with resources known to be available to public authorities;

1.1.2. trustworthy public-key certification authorities and infrastructure;

1.1.3. effective encryption algorithms and parameterisation, such as a minimum of 256-bit key lengths for symmetric encryption, and at least 2048-bit RSA or 256-bit ECC key lengths for asymmetric algorithms.

2. Ensuring ongoing integrity, availability, confidentiality and resilience of processing systems and services

2.1. Futurae enhances the security of processing systems and services in production environments by:

2.1.1. employing a code review process to increase the security of the code used to provide the Services;

2.1.2. testing code and systems for vulnerabilities before and during use;

2.1.3. maintaining an external bug bounty program;

2.1.4. using checks to validate the integrity of encrypted data;

2.1.5. employing preventative and reactive intrusion detection; and

2.1.6. recurring penetration tests against the Futurae applications.

2.2. Futurae deploys high-availability systems utilising multiple availability zones.

2.3. Futurae implements input control measures to protect and maintain the confidentiality of Personal Data, including:

2.3.1. an authorisation policy for input, reading, alteration and deletion of data;

2.3.2. authenticating authorised personnel using unique authentication credentials (passwords) and mandatory multi-factor authentication using security keys;

2.3.3. automatically signing-out user IDs after a period of inactivity;

2.3.4. protecting the input of data, as well as the reading, alteration and deletion of stored data; and

2.3.5. requiring from its hosting providers and personnel that data processing facilities (the rooms housing the computer hardware and related equipment) are kept locked and secure.

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

3.1. Futurae implements measures to ensure that Personal Data is protected from accidental destruction or loss, including by maintaining:

3.1.1. disaster-recovery and business continuity plans and procedures;

3.1.2. applications hosted in multiple availability zones;

3.1.3. redundant infrastructure, including power supplies and internet connectivity;

3.1.4. backups stored encrypted at alternative sites and available for restore in case of failure of primary systems; and

3.1.5. incident management procedures which are regularly tested.

4. Regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

4.1. Futurae's technical and organisational measures are tested and evaluated periodically by external third-party auditors as part of Futurae's Security & Privacy Compliance Program. These may include (i) annual ISO/IEC 27001 audits; and (ii) other external audits. Measures are also regularly tested by internal audits, as well as annual and targeted risk assessments.

5. User identification and authorisation

5.1. Futurae has implemented effective measures for user authentication and privilege management by:

5.1.1. applying the least privilege access principle;

5.1.2. applying a mandatory access control and authentication policy;

5.1.3. applying a zero-trust model of identification and authorisation;

5.1.4. authenticating authorised personnel using unique authentication credentials and strong multi-factor authentication, including requiring the use of physical hard tokens; and

5.1.5. allocating and managing appropriate privileges according to role, approvals, and exception management.

6. Protection of data during transmission

6.1. Futurae has implemented effective measures to protect Personal Data from being copied, read, altered or deleted by unauthorised parties during transmission, including by:

6.1.1. using state-of-the-art transport encryption protocols designed to provide effective protection against active & passive attacks with resources known to be available to public authorities;

6.1.2. using trustworthy public-key certification authorities and infrastructure;

6.1.3. implementing protective measures against active and passive attacks on the sending and receiving systems providing transport encryption, such as adequate firewalls, mutual TLS encryption, API authentication, and encryption to protect the gateways and pipelines through which data travels, as well as testing for software vulnerabilities and possible backdoors;

6.1.4. employing effective encryption algorithms and parameterization, such as a minimum of 256-bit key lengths for symmetric encryption, and at least 2048-bit RSA or 256-bit ECC key lengths for asymmetric algorithms;

6.1.5. using correctly implemented and properly maintained software; and

6.1.6. enforcing secure measures to reliably generate, manage, store and protect encryption keys.

7. Protection of data during storage

7.1. Futurae has implemented effective measures to protect Personal Data during storage, controlling and limiting access to data processing systems, and by:

7.1.1. using state-of-the-art encryption protocols designed to provide effective protection against active and passive attacks with resources known to be available to public authorities;

7.1.2. using trustworthy public-key certification authorities and infrastructure;

7.1.3. testing systems storing data for software vulnerabilities and possible backdoors;

7.1.4. employing effective encryption algorithms and parameterisation, such as requiring all disks storing Personal Data to be encrypted; using correctly implemented and properly maintained software;

7.1.5. enforcing secure measures to reliably generate, manage, store and protect encryption keys;

7.1.6. identifying and authorising systems and users with access to data processing systems;

7.1.7. automatically signing-out users after a period of inactivity; and

7.1.8. audit logging, monitoring, and tracking access to data processing and storage systems.

7.2. Futurae implements access controls to specific areas of data processing systems to ensure only authorised users are able to access the Personal Data within the scope and to the extent covered by their respective access permission (authorisation) and that Personal Data cannot be copied, read, modified or deleted without authorisation. This shall be accomplished by various measures including:

7.2.1. employee policies and training in respect of each employee's access rights to the Personal Data;

7.2.2. applying a zero-trust model of user identification and authorisation;

7.2.3. authenticating authorised personnel using unique authentication credentials and strong multi-factor authentication, including requiring the use of security keys;

7.2.4. monitoring actions of those authorised to delete, add or modify Personal Data;

7.2.5. releasing data only to authorised persons, including the allocation of differentiated access rights and roles; and

7.2.6. controlling access to data, with controlled and documented destruction of data.

8. Physical security of locations at which Personal Data are processed

8.1. Futurae maintains and implements effective physical access control policies and measures in order to prevent unauthorised persons from gaining access to the data processing equipment (namely database and application servers, and related hardware) where the Personal Data are processed or used, including by:

8.1.1. establishing secure areas;

8.1.2. protecting and restricting access paths;

8.1.3. establishing access authorizations for employees and third parties, including the respective documentation;

8.1.4. all access to data hosting environments where Personal Data are hosted are logged, monitored, and tracked; and

8.1.5. data hosting environments where Personal Data are hosted are secured by security alarm systems, and other appropriate security measures.

9. Events logging

9.1. Futurae has implemented a logging and monitoring program to log, monitor and track access to Personal Data, including by system administrators and to ensure data is processed in accordance with instructions received. This is accomplished by various measures, including:

9.1.1. authenticating authorised personnel using unique authentication credentials and strong multi-factor authentication, including the use of security keys;

9.1.2. applying a zero-trust model of user identification and authorisation;

9.1.3. maintaining updated lists of system administrators' identification details;

9.1.4. adopting measures to detect, assess, and respond to high-risk anomalies;

9.1.5. keeping secure, accurate, and unmodified access logs to the processing infrastructure; and

9.1.6. testing the incident response process at least once every 12 months.

10. System configuration, including default configuration

10.1. Futurae maintains configuration baselines for systems supporting the production data processing environment. Automated mechanisms must be used to enforce baseline configurations on production systems, and to prevent unauthorised changes.

10.2. Changes to baselines are limited to a small number of authorised Futurae personnel, and must follow change control processes. Changes must be auditable, and checked regularly to detect deviations from baseline configurations.

10.3. Futurae configures baselines for the information system using the principle of least privilege. By default, access configurations are set to "deny-all" and default passwords must be changed to meet Futurae's

policies prior to device installation on the Futurae network, or immediately after software or operating system installation. Systems are configured to synchronise system time clocks based on International Atomic Time or Coordinated Universal Time (UTC), and access to modify time data is restricted to authorised personnel.

11. Internal IT and IT security governance and management

11.1. Futurae maintains internal policies on the acceptable use of IT systems and general information security.

11.2. Futurae requires all employees to undertake general security and privacy awareness training at least every year. Futurae restricts and protects the processing of Personal Data, and has documented and implemented a formal Information Security Management System (ISMS) in order to protect the integrity, authenticity, confidentiality and availability of Futurae's data and information systems, and to ensure the effectiveness of security controls over data and information systems that support operations.

11.3. Futurae will keep documentation of technical and organisational measures in case of audits and for the conservation of evidence. Futurae shall take reasonable steps to ensure that persons employed by it, and other persons at the place of work concerned, are aware of and comply with the technical and organisational measures set out in this Annex 2.

12. Technical and organisational measures to enable assistance to the controller (and, for transfers from a Processor to a sub-Processor, to the data exporter)

12.1. Futurae considers implementing self-service access to meet data subject requests in exercising their rights of access, erasure, rectification etc. Data subjects are able to login to review and edit Personal Data via the Futurae dashboard.

13. Certification or assurance of processes and products

13.1. The implementation of Futurae's ISMS and related security risk management processes have been externally certified to the industry-standard ISO/IEC 27001 (see certificate).

13.2. Details of other certifications that Futurae may undertake from time to time will be made available on Futurae's website.