Data Processing Addendum

This Data Processing Addendum, including its annexes and the Standard Contractual Clauses, (**DPA**) is made by and between the applicable Xakia entity as defined below (**Xakia**), and Subscriber, pursuant to the Terms of Service for the Services or other written or electronic agreement between the parties (as applicable) (**Agreement**).

This DPA forms part of the Agreement and sets out the terms that apply when Subscriber Personal Data is Processed by Xakia under the Agreement. The purpose of the DPA is to ensure such Processing is conducted in accordance with applicable laws and with due respect for the rights and freedoms of individuals whose Personal Data is Processed.

1. Applicability and Scope

1.1 Applicability

This DPA will apply only to the extent that Xakia Processes, on behalf of Subscriber, Personal Data to which Applicable Data Protection Legislation applies.

1.2 Xakia Contracting Entity

For the purposes of this DPA, **Xakia** means the same Xakia entity that is party to the Agreement with Subscriber, as determined in accordance with the Agreement.

1.3 Scope and Duration

The subject matter of the data Processing is the provision of the Services, and the Processing will be carried out for the duration of the Agreement. Schedule 1 sets out the nature and purpose of the Processing, the types of Personal Data Xakia Processes and the categories of data subjects whose Personal Data is Processed.

This DPA will remain in effect until the later of:

- the expiration or termination of the Agreement; and
- the deletion of Subscriber Personal Data in accordance with Section 9.

1.4 Xakia as a Processor

The parties acknowledge and agree that regarding the Processing of Subscriber Personal Data, Subscriber may act either as a Controller or Processor and Xakia is a Processor. Xakia will Process Subscriber Personal Data in accordance with Subscriber's instructions as set forth in Section 2.1.

1.5 Xakia as a Controller of Account Data

The parties acknowledge that, regarding the Processing of Account Data, Subscriber is a Controller and Xakia is an independent Controller, not a joint Controller with Subscriber. Xakia will Process Account Data as a Controller:

- in order to manage the relationship with Subscriber;
- carry out Xakia's core business operations;
- in order to detect, prevent, or investigate security incidents, fraud, and other abuse or misuse of the Services;
- identity verification;
- to comply with Xakia's legal or regulatory obligations; and
- as otherwise permitted under Applicable Data Protection Legislation and in accordance with this DPA, the Agreement, and the Privacy Policy.

1.6 The parties agree that any notice or communication sent by Xakia to Subscriber shall also satisfy any obligation to send such notice or communication to Subscriber's Affiliate.

2. Xakia as a Processor – Processing Subscriber Personal Data

2.1 Subscriber Instructions

Subscriber appoints Xakia as a Processor to Process Subscriber Personal Data on behalf of, and in accordance with:

- Subscriber's instructions as set forth in the Agreement, this DPA, and as otherwise necessary to provide the Services to Subscriber (which may include investigating security incidents, and detecting and preventing exploits or abuse);
- as necessary to comply with applicable law, including Applicable Data Protection Legislation; and
- as otherwise agreed in writing between the parties,

(**Permitted Purposes**).

2.2 Lawfulness of Instructions

Subscriber will ensure that its instructions comply with Applicable Data Protection Legislation. Subscriber acknowledges that Xakia is neither responsible for determining which laws are applicable to Subscriber's business nor whether Xakia's Services meet or will meet the requirements of such laws. Subscriber will ensure that Xakia's Processing of Subscriber Personal Data, when done in accordance with Subscriber's instructions, will not cause Xakia to violate any applicable law, including Applicable Data Protection Legislation. Xakia will inform Subscriber if it becomes aware, or reasonably believes, that Subscriber's instructions violate applicable law, including Applicable Data Protection Legislation.

2.3 Additional Instructions

Additional instructions outside the scope of the Agreement or this DPA will be mutually agreed to between the parties in writing.

3. Purpose Limitation

Xakia will Process Subscriber Personal Data in order to provide the Services and in accordance with the Agreement. Schedule 1 further specifies the nature and purpose of the Processing, the Processing activities, the duration of the Processing, the types of Personal Data and categories of data subjects.

4. Compliance

Subscriber shall be responsible for ensuring that:

- all such notices have been given, and all such authorizations have been obtained, as required under Applicable Data Protection Legislation, for Xakia (and its Affiliates and Sub-processors) to Process Subscriber Personal Data as contemplated by the Agreement and this DPA;
- it has complied, and will continue to comply, with all applicable laws relating to privacy and data protection, including Applicable Data Protection Legislation; and
- it has, and will continue to have, the right to transfer, or provide access to, Subscriber Personal Data to Xakia for Processing in accordance with the terms of the Agreement and this DPA.

5. Confidentiality

5.1 Confidentiality Obligations of Xakia Personnel.

- **Security Policy and Confidentiality.** Xakia requires all employees to acknowledge in writing, at the time of hire, they will adhere to terms that are in accordance with Xakia's security policies and to protect Subscriber Personal Data at all times. Xakia requires all employees to sign a confidentiality statement at the time of hire.
  Xakia will ensure that any person that it authorizes to Process Subscriber Personal Data (including its staff, agents, and subcontractors) shall be subject to a duty of confidentiality (whether in accordance with Xakia's confidentiality obligations in the Agreement or a statutory duty).
- **Background Checks.** When permitted by law, Xakia will conduct at its expense a criminal background investigation on all employees who are to perform material aspects of the Services under this Agreement.
- **Responding to Third Party Requests.** In the event any Third Party Request is made directly to Xakia in connection with Xakia's Processing of Subscriber Personal Data, Xakia will promptly inform Subscriber and provide details of the same, to the extent legally permitted. Xakia will not respond to any Third Party Request, without prior notice to Subscriber and an opportunity to object, except as legally required to do so or to confirm that such Third Party Request relates to Subscriber.

6. Sub-processors

6.1 Authorization for Sub-processing

Subscriber agrees that:

- Xakia may engage Sub-processors as listed at https://trust.xakiatech.com/ (the **Sub-processor Page**) which may be updated from time to time and Xakia Affiliates; and
- such Affiliates and Sub-processors respectively may engage third party Processors to Process Subscriber Personal Data on Xakia's behalf.

Subscriber provides a general authorization for Xakia to engage onward Sub-processors that is conditioned on the following requirements:

- Xakia will restrict the onward Sub-processor's access to Subscriber Personal Data only to what is strictly necessary to provide the Services and in accordance with the Agreement, and Xakia will prohibit the Sub-processor from Processing the Subscriber Personal Data for any other purpose; and
- Xakia agrees to impose contractual data protection obligations, including appropriate technical and organizational measures to protect Personal Data, on any Sub-processor it appoints that require such Sub-processor to protect Subscriber Personal Data to the standard required by Applicable Data Protection Legislation; and
- Xakia will remain liable and accountable for any breach of this DPA that is caused by an act or omission of its Sub-processors.

6.2 Current Sub-processors and Notification of Sub-processor Additions

- Subscriber understands that effective operation of the Services may require the transfer of Subscriber Personal Data to Xakia Affiliates, or to Xakia's Sub-processors. Subscriber hereby authorizes the transfer of Subscriber Personal Data to locations outside Europe (Xakia's Processing facilities may be located outside Europe depending on Subscriber's selected data location), including to Xakia Affiliates and Sub-processors, subject to continued compliance with this DPA throughout the duration of the Agreement. Subscriber hereby provides general authorization to Xakia engaging additional third-party Sub-processors to Process Subscriber Personal Data in accordance with the Agreement.

- Xakia may, by giving reasonable notice to the Subscriber, add or replace Sub-processors to the Sub-processor Page. Xakia will notify Subscriber if it intends to add or replace Sub-processors from the Sub-processor Page at least thirty (30) days prior to any such changes. Notification will be sent to the Subscriber's Privileged Users by email. If Subscriber reasonably objects to the appointment of a new Sub-processor within thirty (30) days of receiving such notice, on reasonable grounds relating to the protection of the Subscriber Personal Data, then Xakia will work in good faith with Subscriber to find an alternative solution. In the event that the parties are unable to reach a mutually acceptable resolution within a reasonable time thereafter, Subscriber is permitted to terminate the Agreement.

7. Impact Assessments and Consultations

Xakia shall, to the extent required by Applicable Data Protection Legislation, provide Subscriber with reasonable assistance (at Subscriber's cost and expense) with data protection impact assessments or prior consultations with data protection authorities that Subscriber is required to carry out under such legislation.

8. Security

8.1 Xakia has in place and will maintain throughout the term of this Agreement appropriate technical and organizational measures designed to protect Subscriber Personal Data against Security Breaches.

8.2 These measures shall at a minimum comply with applicable law and include the measures identified in Schedule 2.

8.3 Subscriber acknowledges that the security measures are subject to technical progress and development and that Xakia may update or modify the security measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Services purchased by the Subscriber.

8.4 Xakia will ensure that any person authorized to Process Subscriber Personal Data (including its staff, agents, and subcontractors) shall be subject to a duty of confidentiality.

8.5 Upon becoming aware of a Security Breach involving Subscriber Personal Data Processed by Xakia on behalf of Subscriber under this DPA, Xakia shall notify Subscriber without undue delay and shall provide such information as Subscriber may reasonably require, including to enable Subscriber to fulfil its data breach reporting obligations under Applicable Data Protection Legislation.

8.6 Xakia's notification of or response to a Security Breach shall not be construed as an acknowledgement by Xakia of any fault or liability with respect to the Security Breach.

8.7 Subscriber is solely responsible for its use of the Services, including:

- making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of Subscriber Personal Data;
- securing the account authentication credentials, systems and devices Subscriber uses to access the Service; and
- backing up Subscriber Personal Data.

9. Deletion of Subscriber Personal Data

Upon termination or expiry of this Agreement, Xakia will delete all Subscriber Personal Data (including copies) in its possession or control. Unless otherwise agreed, Xakia will automatically delete it from its systems 30 days after the termination or expiration of this Agreement. This will not apply to the extent that Xakia is required by Applicable Data Protection Legislation to retain some or all of the Subscriber Personal Data, which Xakia will securely isolate and protect from any further Processing, except to the extent required by applicable law.

10. Audits

10.1 The parties acknowledge that when Xakia is acting as a Processor on behalf of Subscriber, Subscriber must be able to assess Xakia's compliance with its obligations under Applicable Data Protection Legislation and this DPA.

10.2 Upon written request and at no additional cost to Subscriber, Xakia shall provide Subscriber, and/or its appropriately qualified third-party representative (collectively, the **Auditor**), access to reasonably requested documentation evidencing Xakia's compliance with its obligations under this DPA in the form of the relevant audits or certifications found at https://trust.xakiatech.com/.

10.3 While it is the parties' intention ordinarily to rely on the provision of the documentation to demonstrate Xakia's compliance with this DPA and the provisions of Article 28 of the GDPR, Xakia shall permit Subscriber or its Auditor to carry out an audit, at Subscriber's cost and expense, (including, without limitation, the costs and expenses of Xakia), of Xakia's Processing of Subscriber Personal Data under the Agreement upon Subscriber's written request for an audit, subject to the terms of this Section. Following Xakia's receipt of such request, Xakia and Subscriber shall mutually agree in advance on the details of the audit, including the reasonable start date, scope and duration of any such audit. Any such audit shall be subject to Xakia's security and confidentiality terms and guidelines, may only be performed a maximum of once annually and will be restricted to only data relevant to Subscriber. Where the Auditor is a third-party, Xakia may object in writing to such Auditor, if in Xakia's reasonable opinion, the Auditor is not suitably qualified or is a direct competitor of Xakia. Any such objection by Xakia will require Subscriber to either appoint another Auditor or conduct the audit itself. Any expenses incurred by an Auditor in connection with any review of reports or an audit shall be borne exclusively by the Auditor. For clarity, the exercise of audit rights under the Standard Contractual Clauses shall be as described in this Section.

10.4 Xakia uses external auditors to verify the adequacy of its security measures with respect to its Processing of Subscriber Personal Data. A description of Xakia's certifications and standards for audit can be found at https://trust.xakiatech.com/.

11. Transfer Mechanisms

11.1 Location of Processing

Subscriber acknowledges that Xakia and its Sub-processors may transfer and Process Personal Data to and in the United States of America and other locations in which Xakia, its Affiliates or its Sub-processors maintain data processing operations, as more particularly described in the Sub-processor Page. Xakia shall ensure that such transfers are made in compliance with Applicable Data Protection Legislation and this DPA.

11.2 Transfer Mechanism

The parties agree that when the transfer of Personal Data from Subscriber (as "data exporter") to Xakia (as "data importer") is a Restricted Transfer, Applicable Data Protection Legislation requires that appropriate safeguards are put in place. For the purposes of such Restricted Transfers from Subscriber to Xakia, such transfer shall be subject to the appropriate Standard Contractual Clauses, which shall be deemed incorporated into and form part of this DPA, as follows:

- In relation to transfers of Subscriber Personal Data that is protected by the GDPR, the EU SCCs shall apply, completed as follows:
  - Module Two or Module Three will apply (as applicable);
  - in Clause 7, the optional docking clause will apply;
  - in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-processor changes shall be as set out in section 6.2;
  - in Clause 11, the optional language will not apply;
  - in Clause 17, Option 1 will apply, and the EU SCCs will be governed by the law of the EU Member State in which the data exporter is established and if no such law by Irish law;
  - in Clause 18(b), disputes shall be resolved before the courts of the EU Member State in which the data exporter is established and otherwise Ireland;
  - Annex I of the EU SCCs shall be deemed completed with the information set out in Schedule 1;
  - subject to Section 8.3, Annex II of the EU SCCs shall be deemed completed with the information set out in Schedule 2; and
  - Annex III of the EU SCCs shall be deemed completed with the information set out in Schedule 3; and
- In relation to transfers of Account Data protected by the GDPR and Processed in accordance with Section 1.5, the EU SCCs shall apply, completed as follows:
  - Module One will apply;
  - in Clause 7, the optional docking clause will apply;
  - in Clause 11, the optional language will not apply;
  - in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;
  - in Clause 18(b), disputes shall be resolved before the courts of Ireland;
  - Annex I of the EU SCCs shall be deemed completed with the information set out in Schedule 1; and
  - Subject to Section 8.3, Annex II of the EU SCCs shall be deemed completed with the information set out in Schedule 2; and
  - Annex III of the EU SCCs shall be deemed completed with the information set out in Schedule 3; and
- In relation to transfers of Personal Data protected by the UK GDPR or Swiss DPA, the EU SCCs as implemented under the first and second bullet points above will apply with the following modifications:
  - references to "Regulation (EU) 2016/679" shall be interpreted as references to UK Data Protection Laws or the Swiss DPA (as applicable);
  - references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of UK Data Protection Laws or the Swiss DPA (as applicable);
  - references to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to "UK" or "Switzerland", or "UK law" or "Swiss law" (as applicable);
  - the term "member state" shall not be interpreted in such a way as to exclude data subjects in the UK or Switzerland from the possibility of suing for their rights in their place of habitual residence (i.e., the UK or Switzerland);
  - Clause 13(a) and Part C of Annex I are not used and the "competent supervisory authority" is the UK Information Commissioner or Swiss Federal Data Protection Information Commissioner (as applicable);
  - references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Information

Commissioner" and the "courts of England and Wales" or the "Swiss Federal Data Protection Information Commissioner" and "applicable courts of Switzerland" (as applicable);

  - in Clause 17, the Standard Contractual Clauses shall be governed by the laws of England and Wales or Switzerland (as applicable); and
  - with respect to transfers to which UK Data Protection Laws apply, Clause 18 shall be amended to state "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may bring legal proceeding against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts", and with respect to transfers to which the Swiss DPA applies, Clause 18(b) shall state that disputes shall be resolved before the applicable courts of Switzerland.

- To the extent that and for so long as the EU SCCs as implemented in accordance with the first, second and third bullet points above cannot be used to lawfully transfer Subscriber Personal Data and Account Data in accordance with the UK GDPR to Xakia, the UK SCCs shall be incorporated into and form an integral part of this DPA and shall apply to transfers governed by the UK GDPR. For the purposes of the UK SCCs, the relevant annexes, appendices or tables shall be deemed populated with the information set out in Schedules 1 and 2.
- It is not the intention of either party to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses and, accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of the Agreement (including this DPA) the Standard Contractual Clauses shall prevail to the extent of such conflict.

11.3 Alternative Transfer Mechanism

To the extent that Xakia adopts an alternative data export mechanism (including any new version of or successor to the Standard Contractual Clauses adopted pursuant to Applicable Data Protection Legislation) (**Alternative Transfer Mechanism**), the Alternative Transfer Mechanism shall upon notice to Subscriber and an opportunity to object of no less than 30 days, apply instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with Applicable Data Protection Legislation applicable to Europe and extends to territories to which Subscriber Personal Data and Account Data is transferred).

12. Cooperation and Data Subject Rights

12.1 Data Subject Rights

Xakia provides Subscriber with a number of self-service features via the Services, including the ability to delete, obtain a copy of, or restrict use of Subscriber Data. Subscriber may use such self-service features to assist in complying with its obligations under Applicable Data Protection Law with respect to responding to Third Party Requests from data subjects via the Services at no additional cost. Upon Subscriber's request, Xakia shall, taking into account the nature of the Processing, provide reasonable assistance to Subscriber where possible and at Subscriber's cost and expense, to enable Subscriber to respond to requests from a data subject seeking to exercise their rights under Applicable Data Protection Legislation. In the event that such request is made directly to Xakia, if Xakia can, through reasonable means, identify the Subscriber as the Controller of the Subscriber Personal Data of a data subject, Xakia shall promptly inform Subscriber of the same. As between the parties, Subscriber shall have sole discretion and responsibility in responding to the rights asserted by any individual in relation to Subscriber Personal Data.

12.2 Cooperation

In the event that either party receives:

- any request from a data subject to exercise any of its rights under Applicable Data Protection Legislation; or
- any Third Party Request relating to the Processing of Account Data or Subscriber Personal Data conducted by the other party,

such party will promptly inform the other party in writing. The parties agree to cooperate, in good faith, as necessary to respond to any Third Party Request and fulfill their respective obligations under Applicable Data Protection Legislation.

13. No Sale or Sharing

To the extent that the Processing of Subscriber Personal Data is subject to U.S. data protection laws, Xakia is prohibited from:

- selling Subscriber Personal Data or otherwise making Subscriber Personal Data available to any third party for monetary or other valuable consideration;
- sharing Subscriber Personal Data with any third party for cross-behavioral advertising;
- retaining, using, or disclosing Subscriber Personal Data for any purpose other than for the business purposes specified in this DPA or as otherwise permitted by U.S. data protection laws;
- retaining, using or disclosing Subscriber Personal Data outside of the direct business relationship between the parties, and;
- except as otherwise permitted by U.S. data protection laws, combining Subscriber Personal Data with Personal Data that Xakia receives from or on behalf of

another person or persons, or collects from its own interaction with the data subject.

Xakia will notify Subscriber promptly if it makes the determination that it can no longer meet its obligations under applicable U.S. data protection laws.

14. Miscellaneous

14.1 If there is a conflict between the Agreement and this DPA, the terms of this DPA will prevail. The order of precedence will be: (a) this DPA; (b) the Agreement; and (c) the Privacy Policy. To the extent there is any conflict between the Standard Contractual Clauses, and any other terms in this DPA, the Agreement, or the Privacy Policy, the provisions of the Standard Contractual Clauses will prevail.

14.2 The parties agree that this DPA shall replace and supersede any prior data processing addendum that Xakia and Subscriber may have previously entered into in connection with the Services.

14.3 Any claims brought in connection with this DPA will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations set forth in the Agreement.

14.4 In no event does this DPA restrict or limit the rights of any data subject or of any competent supervisory authority.

14.5 In the event (and to the extent only) of a conflict (whether actual or perceived) among Applicable Data Protection Legislation, the parties (or relevant party as the case may be) shall comply with the more onerous requirement or standard which shall, in the event of a dispute in that regard, be solely determined by Xakia.

14.6 Notwithstanding anything else to the contrary in the Agreement and without prejudice to Sections 1.4 and 1.5, Xakia reserves the right to make any modification to this DPA as may be required to comply with Applicable Data Protection Legislation. Xakia will provide Subscriber with at least thirty (30) days' notice of such amendments, during which time the Subscriber may reasonably object. The parties will work together in good faith to agree on any measures required to ensure compliance with the law.

14.7 Notwithstanding anything in the Agreement or any order form entered in connection therewith, the parties acknowledge and agree that Xakia access to Subscriber Personal Data does not constitute part of the consideration exchanged by the parties in respect of the Agreement.

14.8 In no event shall this DPA benefit or create any right or cause of action on behalf of a third party (including a Third-Party Controller), but without prejudice to the rights or remedies available to Data Subjects under Data Protection Laws or this DPA (including the Standard Contractual Clauses).

15. Definitions

Terms used in this DPA have the meanings given to the Agreement and the following terms have the following meanings:

Account Data	Personal Data that relates to Subscriber's or any User’s relationship with Xakia.
Applicable Data Protection Legislation	Laws and regulations applicable to Xakia's Processing of Personal Data under the Agreement, including but not limited to: • the GDPR; • in respect of the UK, the GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2019 (**UK GDPR**) and the Data Protection Act 2018 (together, **UK Data Protection Laws**); • the Swiss Federal Data Protection Act and its implementing regulations (**Swiss DPA**); • CCPA & CPRA; and • Australian Privacy Principles and the Australian Privacy Act (1988), in each case, as may be amended, superseded or replaced.
CCPA or **CCPA and CPRA**	The California Consumer Privacy Act of 2018, the California Privacy Rights Act of 2020, and any binding regulations promulgated thereunder, in each case, as may be amended from time to time.
Controller	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. It shall have the same meaning ascribed to "controller" under the GDPR and other equivalent terms under Applicable Data Protection Legislation (e.g., "Business" as defined under the CCPA), as applicable.
Europe	The European Economic Area (**EEA**), the United Kingdom (**UK**) and Switzerland, or another country which ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of Personal Data, as determined by the European Commission in the case that EU Data Protection Law applies respectively as determined by the ICO in the case that UK Data Protection Law applies.
GDPR	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).
Personal Data	Any information, including personal information, relating to an identified or identifiable natural person ("data subject") or as defined in and subject to Applicable Data Protection Legislation.
Privacy Policy	Xakia's current privacy policy available at the applicable link as set forth in the Agreement.
Processor	The entity which Processes Personal Data on behalf of the Controller. It shall have the meaning ascribed to "processor" under the GDPR and other equivalent terms under other Applicable Data Protection Legislation (e.g., "Service Provider" as defined under the CCPA), as applicable.
Processing (and **Process**)	Any operation or set of operations performed upon Personal Data, whether or not by automated means, such as collection, recording, securing, organization, storage, adaptation or alteration, access to, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.
Restricted Transfer	• where the GDPR applies, a transfer of Personal Data from the EEA to a country outside of the EEA which is not subject to an adequacy determination by the European Commission; • where the UK GDPR applies, a transfer of Personal Data from the UK to any other country which is not based on adequacy regulations pursuant to Section 17A of the Data Protection Act 2018; and • where the Swiss DPA applies, a transfer of Personal Data to a country outside of Switzerland which is not included on the list of adequate jurisdictions published by the Swiss Federal Data Protection and Information Commissioner.
Security Breach	A breach of security leading to any accidental, unauthorized or unlawful loss, disclosure, destruction, loss, alteration, unauthorized disclosure of, or access to Subscriber Personal Data transmitted, stored or otherwise Processed by Xakia. A Security Incident shall not include an unsuccessful attempt or activity that does not compromise the security of Subscriber Personal Data, including (without limitation) pings and other broadcast attacks of firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents.
Services	The services provided by Xakia to Subscriber under the Agreement.
Standard Contractual Clauses	• Where the GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision (EU) 2021/914 of 4 June 2021 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, available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN (**EU SCCs**); or • where the UK GDPR applies, the applicable standard data protection clauses adopted pursuant to Article 46(2)(c), or where the UK GDPR means the International Data Transfer Addendum to the EU Standard Contractual Clauses issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018, as such Addendum may be revised under Section 18 therein (**UK SCCs**); or • where the Swiss DPA applies, the applicable standard data protection clauses issued, approved or recognized by the Swiss Federal Data Protection and Information Commissioner (the **Swiss SCCs**), in each case, as updated, amended or superseded from time to time.
Sub-processor	• Xakia, when Xakia is Processing Subscriber Personal Data and where Subscriber is itself a Processor of such Subscriber Personal Data; or • any third-party Processor engaged by Xakia or its Affiliates to assist in fulfilling Xakia's obligations under the Agreement and which Processes Subscriber Personal

	Data. Sub-processors may include third parties or Xakia Affiliates but shall exclude Xakia employees, contractors or consultants.
Subscriber Personal Data	Personal Data that Xakia Processes as a Processor on behalf of Subscriber.
Terms of Service	• in relation to the Xakia Platform, the terms of service available at: https://www.xakiatech.com/terms-of-service; and/or • in relation to Xakia Connect, the ters of service available at: https://www.xakiatech.com/connect-legal.
Third Party Request	any request, correspondence, inquiry, or complaint from a data subject, regulatory authority, or third party.
UK Addendum	The International Data Transfer Addendum to the EU Standard Contractual Clauses issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018, as such Addendum may be revised under Section 18 therein. This is found in Schedule 4 below.

Schedule 1

Details of Processing

Annex I

A. List of Parties

Data exporter(s): *[Identity and contact details of the controller(s) /data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name of Data exporter:	The party identified as the "Subscriber" in the Agreement and this DPA
Address:	As set forth in the Agreement
Contact person's name, position, and contact details:	As set forth in the Agreement
Activities relevant to the data transferred under these Clauses:	See Annex 1(B) below
Signature and date:	This Annex I shall automatically be deemed executed when the Agreement is executed by Subscriber
Role (controller/processor):	Controller or Processor

Data importer(s): *[Identity and contact details of the processor(s) /data importer(s), including any contact person with responsibility for data protection]*

Name:	As set forth in the Agreement
Address:	As set forth in the Agreement
Contact person's name, position, and contact details:	Xakia Privacy Team – legal@xakiatech.com
Signature and date:	This Annex I shall automatically be deemed executed when the Agreement is executed by Xakia
Role (controller/processor):	Processor

B. Description of Processing/Transfer

Categories of Data Subjects whose Personal Data is transferred	**Module One** Users **Modules Two and Three** Subscriber’s Users, other employees and other other data subjects whose Personal Data is Processed in connection with Subscriber's use of the Services (for example, by virtue of their Personal Data being included in a legal matter or contract).
Categories of Personal Data transferred	**Module One** Account Data which constitutes Personal Data, such as name and email address. **Modules Two and Three** Any Subscriber Personal Data Processed by Xakia in connection with the Services including but not limited to legal matter data, contract information, documents, email communications, name, contact information, and other data uploaded to or created within the Services.
Sensitive data transferred (if applicable) and	Xakia does not knowingly collect any sensitive data or any special categories of data (as defined under Applicable Data Protection Legislation). The Services are not designed for handling Sensitive Data.

applied restrictions or safeguards	
Frequency of the transfer	Continuous
Nature and purpose(s) of the data transfer and Processing	**Module One** Personal data contained in Account Data will be Processed to manage the account, including to access Subscriber's or any User's account, for identity verification, to maintain or improve the performance of the Services, to provide support, to investigate and prevent system abuse, or to fulfill legal obligations. **Modules Two and Three** Personal Data contained in Subscriber Personal Data will be Processed as necessary to provide the Services and in accordance with the Agreement, or to fulfil legal obligations.
Retention period (or, if not possible to determine, the criteria used to determine the period)	**Module One** Xakia will Process Account Data as long as required: • to provide the Services to Subscriber; • for Xakia's lawful and legitimate business needs; or • in accordance with applicable law or regulation. Account Data will be stored in accordance with the Privacy Policy. **Modules Two and Three** Upon termination or expiry of this Agreement, Xakia will delete all Subscriber Personal Data (including copies) in its possession or control. Subscriber may request to Xakia to delete all Subscriber Personal Data, and Xakia will proceed to delete the data as soon as reasonably practicable and within a maximum period of 30 days from Subscriber's written request. If Subscriber does not request deletion of Subscriber Personal Data, Xakia will automatically delete it from our systems 30 days after the termination or expiration of this Agreement. This will not apply to the extent that Xakia is required by law to retain some or all of the Subscriber Personal Data, which Xakia will securely isolate and protect from any further Processing, except to the extent required by applicable law.
For transfers to (sub-) processors, also specify subject matter, nature, and duration of the Processing	**Modules Two and Three only** Xakia will restrict the onward Sub-processor's access to Subscriber Personal Data only to what is strictly necessary to provide the Services and in accordance with the Agreement, and Xakia will prohibit the Sub-processor from Processing the Personal Data for any other purpose. Xakia imposes contractual data protection obligations, including appropriate technical and organizational measures to protect Personal Data, on any Sub-processor it appoints that require such Sub-processor to protect Subscriber Personal Data to the standard required by Applicable Data Protection Legislation. Xakia will remain liable and accountable for any breach of this DPA that is caused by an act or omission of its Sub-processors.
Identify the competent supervisory authority/ies in accordance with Clause 13	Where the EU GDPR applies the competent supervisory authority shall be: • the supervisory authority applicable to the data exporter in its EEA country of establishment; or • where the data exporter is not established in the EEA, the supervisory authority applicable in the EEA country where the data exporter's EU representative has been appointed pursuant to Article 27(1) GDPR; or • where the data exporter is not obliged to appoint a representative, the supervisory authority applicable to the EEA country where the data subjects relevant to the transfer are located. Where the UK GDPR applies, the UK Information Commissioner's Office.

Schedule 2

Technical and Organizational Security Measures

Annex II

Further details of Xakia's technical and organizational security measures to protect Subscriber Data are available at: https://trust.xakiatech.com/

Where applicable, this Schedule 2 will serve as Annex II to the Standard Contractual Clauses. The following table provides more information regarding the technical and organizational security measures:

Technical and Organizational Security Measure	Evidence of Technical and Organizational Security Measure
Measures of pseudonymisation and encryption of personal data	Xakia makes HTTPS encryption (also referred to as SSL or TLS) available on the service using industry standard algorithms and certificates. Xakia has implemented technologies to ensure that stored data is encrypted at rest.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Xakia implements industry standard access controls and detection capabilities including ISO 27001 certification. Infrastructure providers use commercially reasonable efforts to ensure a minimum of 99.9% uptime. Backup and replication strategies are designed to ensure redundancy and fail-over protections.
Measures for 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	Subscriber data is backed up to data stores and replicated across multiple availability zones. Xakia's products are designed to ensure redundancy and seamless failover. The server instances are architected with a goal to prevent single points of failure.
Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	Xakia maintains relationships with industry recognized penetration testing service providers for annual penetration tests. Security reviews of code stored in Xakia's source code repositories is performed, checking for coding best practices and identifiable software flaws.
Measures for user identification and authorisation	Xakia maintains a uniform password policy for its customers. The authorisation model is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options. Public product APIs may be accessed using an API key or through OAuth authorization.
Measures for the protection of data during transmission	Xakia makes HTTPS encryption (also referred to as SSL or TLS) available on the service. Xakia's HTTPS implementation uses industry standard algorithms and certificates.
Measures for the protection of data during storage	Xakia stores user passwords following policies that follow industry standard practices for security. Xakia has implemented technologies to ensure that stored data is encrypted at rest.
Measures for the protection of data during storage	Xakia stores user passwords following policies that follow industry standard practices for security. Xakia has implemented technologies to ensure that stored data is encrypted at rest.
Measures for ensuring physical security of locations at which personal data are processed	Xakia hosts its product infrastructure with multitenant, outsourced infrastructure providers. The physical and environmental security controls are SOC 2 Type II and ISO 27001 compliant, among other certifications.
Measures for ensuring events logging	Xakia designed its infrastructure to log extensive information about the system behaviour, traffic received, system authentication, and other application requests. Internal systems

	aggregated log data and alert appropriate employees of malicious, unintended, or anomalous activities.
Measures for ensuring system configuration, including default configuration	Xakia maintains a uniform password policy and implements industry standard access controls. The authorisation model ensures appropriate access controls are maintained across the system configuration.
Measures for internal IT and IT security governance and management	All Xakia employees undergo a background check prior to being extended an employment offer, in accordance with applicable laws. Employee roles are reviewed at least once per annum. A subset of Xakia's employees have access to customer data via controlled interfaces for support, troubleshooting, and security incident response.
Measures for certification/assurance of processes and products	Xakia maintains ISO 27001 and SOC 2 Type II certification. Xakia uses external auditors to verify the adequacy of its security measures.
Measures for ensuring data minimisation	A subset of Xakia's employees have access to customer data via controlled interfaces only to the extent necessary to provide effective customer support, troubleshoot problems, detect and respond to security incidents and implement data security.
Measures for ensuring data quality	Xakia designed its infrastructure to log extensive information and alert appropriate employees of malicious, unintended, or anomalous activities that could affect data quality.
Measures for ensuring limited data retention	As specified in Section 9, Subscriber Personal Data is automatically deleted 30 days after termination of the Agreement unless Subscriber requests earlier deletion.
Measures for ensuring accountability	Employee roles are reviewed at least once per annum. All employees are required to conduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards. Background checks are conducted when permitted by law.
Measures for allowing data portability and ensuring erasure	Subscriber may use self-service features via the Services to delete, obtain a copy of, or restrict use of Subscriber Personal Data as described in Section 12.
Technical and organizational measures to be taken by the [sub]-processor to provide assistance to the controller and, for transfers from a processor to a [sub]-processor, to the Subscriber.	Xakia imposes contractual data protection obligations, including appropriate technical and organizational measures to protect personal data, on any Sub-processor it appoints that require such Sub-processor to protect Subscriber Personal Data to the standard required by Applicable Data Protection Legislation as described in Section 6.

Schedule 3

Sub-processors

Annex III

In Clause 9 of the 2021 Standard Contractual Clauses, Option 2 will apply and the time period for prior notice of Sub-processor changes will be as set forth in Section 6.2.

Subscriber agrees that:

- Xakia may engage Xakia Affiliates and Sub-processors as listed on the Sub-processor Page; and
- Xakia may, by giving reasonable notice to the Subscriber, add or replace a Sub-processors from the Sub-processor Page at least thirty (30) days prior to any such changes. Notification will be sent to the Subscriber's Privileged Users by email. If Subscriber reasonably objects to the appointment of a new Sub-processor within thirty (30) days of receiving such notice, on reasonable grounds relating to the protection of the Subscriber Personal Data, then Xakia will work in good faith with Subscriber to find an alternative solution. In the event that the parties are unable to reach a mutually acceptable resolution within a reasonable time thereafter, Subscriber is permitted to terminate the Agreement.

Schedule 4

UK Addendum

1. **Date of this Addendum:** This Addendum is effective from the same date as the DPA.
2. **Background:** The Information Commissioner considers this Addendum to provide appropriate safeguards for the purposes of transfers of personal data to a third country or an international organisation in reliance on Articles 46 of the UK GDPR and, with respect to data transfers from controllers to processors and/or processors to processors.
3. **Interpretation of this Schedule 4:** Where this Addendum uses terms that are defined in the Annex those terms shall have the same meaning as in the Annex. In addition, the following terms have the following meanings:

This Addendum	This Addendum to the Clauses
The Annex	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	The United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.
UK	The United Kingdom of Great Britain and Northern Ireland.

4. This Addendum shall be read and interpreted in the light of the provisions of UK Data Protection Laws, and so that it fulfils the intention for it to provide the appropriate safeguards as required by Article 46 GDPR.
5. This Addendum shall not be interpreted in a way that conflicts with rights and obligations provided for in UK Data Protection Laws.
6. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.
7. Hierarchy: In the event of a conflict or inconsistency between this Addendum and the provisions of the Clauses or other related agreements between the Parties, existing at the time this Addendum is agreed or entered into thereafter, the provisions which provide the most protection to data subjects shall prevail.
8. **Incorporation of the Clauses:** This Addendum incorporates the Clauses which are deemed to be amended to the extent necessary so they operate:
    a. for transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that transfer; and
    b. to provide appropriate safeguards for the transfers in accordance with Articles 46 of the UK GDPR Laws.
9. The amendments required by Section 7 above, include (without limitation):
    a. References to the "Clauses" means this Addendum as it incorporates the Clauses.
    b. Clause 6 Description of the transfer(s) is replaced with: "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer".
    c. References to "Regulation (EU) 2016/679" or "that Regulation" are replaced by "UK Data Protection Laws" and references to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws.

d. References to Regulation (EU) 2018/1725 are removed.

e. References to the "Union", "EU" and "EU Member State" are all replaced with the "UK".

f. Clause 13(a) and Part C of Annex II are not used; the "competent supervisory authority" is the Information Commissioner.

g. Clause 17 is replaced to state "These Clauses are governed by the laws of England and Wales".

h. Clause 18 is replaced to state: "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."

i. The footnotes to the Clauses do not form part of the Addendum.

10. **Amendments to this Addendum**

a. The Parties may agree to change Clause 17 and/or 18 to refer to the laws and/or courts of Scotland or Northern Ireland.

b. The Parties may amend this Addendum provided it maintains the appropriate safeguards required by Art 46 UK GDPR for the relevant transfer by incorporating the Clauses and making changes to them in accordance with Section 7 above.

11. **Executing this Addendum**: The Parties may enter into the Addendum (incorporating the Clauses) in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in the Clauses. This includes (but is not limited to):

a. By attaching this Addendum as Schedule 4 to the DPA.

b. By adding this Addendum to the Clauses and including in the following above the signatures in Annex 1A:

"By signing we agree to be bound by the UK Addendum to the EU Commission Standard Contractual Clauses dated:" and add the date (where all transfers are under the Addendum)

"By signing we also agree to be bound by the UK Addendum to the EU Commission Standard Contractual Clauses dated" and add the date (where there are transfers both under the Clauses and under the Addendum)

(or words to the same effect) and executing the Clauses; or

c. By amending the Clauses in accordance with this Addendum and executing those amended Clauses.