GLOBAL DATA PRIVACY ADDENDUM

This Global Data Privacy Addendum (this "**Privacy Addendum**") is attached and made part of the agreement (the **"Master Agreement**") between Customer (as identified on the Quote or the Master Agreement), including all affiliates, if any, and Khoros, LLC ("Khoros" or "Service Provider").

Unless otherwise stated, the terms of this Privacy Addendum will apply to all processing of Personal Data on behalf of the Customer in relation to the Services provided under the terms of the Master Agreement.

1. DEFINITIONS

1.1 "**Adequate Country**" means a country or territory recognised as providing an adequate level of protection for Personal Data under an adequacy decision made, from time to time, by (as applicable) (i) the Information Commissioner's Office and/or under applicable UK law (including the UK GDPR), or (ii) the European Commission under the GDPR, or (iii) the Swiss Federal Data Protection Authority under Swiss Data Protection Law.

1.2 **"CCPA"** means the California Consumer Privacy Act, Cal Civ. Code 1798.100 *et seq.*, as amended

1.3 "**Data Protection Laws**" means, as applicable, the EU/UK Rules, the Swiss Data Protection Law, the CCPA, and other applicable data processing and privacy laws that require contractual terms for the processing or international transfer of Personal Data, provide for breach notifications of a Security Breach, or authorize Data Subject Requests.

1.4 **"Data Subject Request**" means a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure, data portability, object to the processing, right not to be subject to an automated individual decision making, or other data subject right provided for in the Data Protection Laws**.**

1.5 "**EEA**" means the European Economic Area.

1.6 "**EU Clauses**" means the standard contractual clauses for international transfers of personal data to third countries set out in the European Commission's Decision 2021/914 of 4 June 2021 (at http://data.europa.eu/eli/dec_impl/2021/914/oj) incorporating Module Two for Controller to Processor transfers and Module Three for Processor to Processor transfers (as applicable), or its valid successor, and which form part of this Privacy Addendum in accordance with Schedule 4.

1.7 **"EU/UK Rules"** means (a) in the European Union, the General Data Protection Regulation 2016/679 (the "**GDPR**"), (b) in the UK, the UK General Data Protection Regulation 2016/679, as implemented by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 and the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020 (the "**UK GDPR**") and the Data Protection Act 2018.

1.8 **"Personal Data**" means (i) any information relating to an identified or identifiable natural person ('**Data Subject'**) located in the EEA, United Kingdom ("**UK**") or Switzerland; an identifiable natural person is one who can be identified, directly or indirectly in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; and (ii) as defined as "personal data" or "personal information" under the Data Protection Laws; and in each case, is processed by Service Provider on behalf of the Customer within the scope of the Master Agreement. For clarity, unless otherwise expressly agreed in writing herein, the parties acknowledge that Service Provider does not process any Personal Data in connection with on premises software sold by Service Provider and hosted by Customer or Customer's data center.

1.9 "**Security Breach**" means,(i) under GDPR, any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data by Service Provider; or (ii) any other incident concerning Personal Data requiring breach notification under the Data Protection Laws.

1.10 **"Services"** means the services and other activities to be supplied to or carried out by or on behalf of Service Provider for the Customer pursuant to the Master Agreement.

1.11 **"Standard Contractual Clauses"** means the EU Clauses, the Swiss Addendum and/or the UK Approved Addendum.

1.12 "**Supervisory Authority**" means in the UK, the Information Commissioner's Office ("**ICO**") (and, where applicable, the Secretary of State or the government), and in the EEA, an independent public authority established pursuant to the GDPR.

1.13 "**Swiss Addendum**" means the addendum set out in Schedule 3.

1.14 "**Swiss Data Protection Law**" means the Swiss Federal Data Protection Act of 19 June 1992 and the Swiss Federal Data Protection Act of 25 September 2020 and its corresponding ordinances as amended, superseded or replaced from time to time.

1.15 "**UK Approved Addendum**" means the template Addendum B.1.0 issued by the UK's Information Commissioner's Office and laid before Parliament in accordance with s119A of the Data Protection Act 2018 of the UK on 2 February 2022, and in force on 21 March 2022, or its valid successor.

1.16 **"UK Mandatory Clauses**" means the Mandatory Clauses of the UK Approved Addendum, as updated from time to time and/or replaced by any final version published by the Information Commissioner's Office.

1.17 Capitalized terms used but not defined in this Privacy Addendum have the meanings assigned to them in the Master Agreement or the Data Protection Laws, including the terms "Data Protection Officer", "Member States", "Personal Data Breach", "Privacy Impact Assessment".

2. APPLICABILITY; ROLES OF THE PARTIES

2.1 This Privacy Addendum amends and supplements the Master Agreement between the parties.

2.2 Customer is the controller or processor of Personal Data, and Service Provider is the processor or sub-processor of Personal Data. Each party will comply (and will procure that any of its personnel comply and use commercially reasonable efforts to procure that its sub-processors comply), with Data Protection Laws applicable to such party in the processing of Personal Data. Customer shall ensure its instructions to Service Provider comply with all Data Protection Laws applicable in relation to the Personal Data, and that the instructions will not cause Service Provider to be in breach of the Data Protection Laws. As between the parties, Customer shall have sole responsibility for (a) the accuracy, quality, and legality of Personal Data; (b) the means by which the Personal Data was acquired; (c) ensuring the Services are appropriate for Customer as well as its Personal Data, and the processing lawful under the Data Protection Laws; (d) ensuring any required consent of a Data Subject is obtained; and (e) establishing and maintaining the applicable information security safeguards and policies for protecting Personal Data in Customer's facilities and data centers.

2.3 Social Media Content (Each Party a Data Controller). Khoros and Customer are each independent Controllers over the Personal Data included in or derived from social media platforms to the extent a copy of that data is Processed or stored by the Applications. Each party agrees to use content from social media platforms strictly in accordance with any applicable terms of service that a social media platform imposes and any Data Protection Law provisions applicable to Data Controllers. To the extent Customer transfers any Personal Data contained in Social Media Content (as that term is defined in the Master Agreement) to any country outside the EEA (except a country that is recognized under Data Protection Laws from time to time as providing adequate protection for Personal Data), the parties agree that the EC Standard Contractual Clauses – Controller to Controller (the "Controller to Controller Clauses") will apply in respect of such transfer and that Khoros will comply with the obligations of the data exporter, and Customer with the obligations of the data importer, set forth in the Controller to Controller Clauses. The Controller to Controller Clauses are incorporated into and made part of this Privacy Addendum. Further, if Data

Protection Laws requires or Customer requests, Khoros will sign physical copies of the Controller to Controller Clauses.

3. DESCRIPTION OF PROCESSING

3.1 The subject matter, nature and purposes of the processing. duration, types of Personal Data and categories of Data Subject are as set out in Schedule 1.

3.2 *Processing by Service Provider.* As a processor, Service Provider will only process Personal Data (i) in order to provide the Services to Customer or (ii) per Customer's reasonable instructions in writing or via the Services. Service Provider will notify Customer (unless prohibited by applicable law) if it is required under applicable law to process Personal Data other than pursuant to Customer's instructions. As soon as reasonably practicable upon becoming aware, inform the Customer if, in Service Provider's opinion, any instructions provided by the Customer under section 3 infringe applicable Data Protection Laws. Upon termination of the Master Agreement , return (upon written request of the Customer prior to termination) or delete the Personal Data, unless required by law to continue to store a copy of any Personal Data. If Customer is a processor, Customer shall on an ongoing basis ensure that the relevant controller has authorized its instructions to Service Provider and Customer's engagement of Service Provider as another processor.

3.3 Service Provider is licensed to use the Personal Data for the Services for the term of and in accordance with this Privacy Addendum. To the extent that the provisions of the Master Agreement or the instructions of the Customer necessitate the copying, disclosure or processing of data, this will be deemed to constitute the required authority to do so.

4. TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

4.1 Service Provider will implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks that are presented by the processing of Personal Data, in particular protection against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data as set out in Schedule 5. Service Provider has no obligation to assess Personal Data in order to identify information subject to any specific legal requirements. Service Provider may update the security measures from time to time provided that such updates do not result in a material reduction of the security of the Services. The Services may offer Customer additional options to secure Personal Data ("Security Options").

4.2 Service Provider will take reasonable steps to ensure that only authorized personnel have access to Personal Data and that any persons whom it authorizes to access the Personal Data on its behalf are under obligations of confidentiality.

4.3 Customer is responsible for its use of the Services and its storage of any copies of Personal Data outside Service Provider's or Service Provider's Subprocessors' systems, including (i) using the Services and Security Options to ensure a level of security appropriate to the risk to the Personal Data; (ii) securing the account authentication credentials, systems and devices Customer uses to access the Services; and backing up or retaining copies of its Personal Data as appropriate. Customer agrees that the Services, security measures, and Security Options provide a level of security appropriate to the risk to Personal Data, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of Personal Data as well as the risks to individuals.

5. SUB-PROCESSING

5.1 Customer grants a general authorisation to Service Provider to appoint its Affiliates or third parties as sub-processors to support the performance of the Services, including but not limited to data centre operators, cloud-based software providers, and other outsourced support and service providers. Such authorization includes offshore entities who employ foreign nationals, as well as

employees and contractors of Service Provider's affiliates and subsidiaries, who may also be foreign nationals, in performance of its obligations described in the Master Agreement, and Service Provider has the right to disclose Personal Information to such third parties provided that such third parties are subject to confidentiality obligations similar to those between Service Provider and Customer.

5.2 Service Provider will maintain a list of sub-processors, available to Customer at https://khoros.com/khoros-subprocessors, and will add the names of new and replacement sub-processors to the list prior to them starting sub-processing of Personal Data. To the extent required by Data Protection Laws, if Customer has a reasonable objection to any new or replacement sub-processor, it shall notify Service Provider of such objections in writing within 15 days and the parties will seek to resolve the matter in good faith. Customer may not unreasonably object to the subprocessor. Service Provider may use a new or replacement sub-processor (i) whilst the objection procedure in this section 5.2 is in process; or (ii) on an emergency basis if necessary. If it can be reasonably demonstrated to Service Provider that the new subprocessor is unable to process Personal Data in compliance with Data Protection Laws and Service Provider cannot provide an alternative subprocessor, of it the parties are not otherwise able to achieve resolution, to the extent feasible, Service Provider shall quote an additional fee to Customer to resolve the objection.

5.3 To the extent required by Data Protection Laws, Service Provider will enter into a written contract with each sub-processor which imposes on such sub-processor terms no less protective of Personal Data than those imposed on Service Provider in this Privacy Addendum (the "Relevant Terms"). Service Provider shall be liable to Customer for any breach by such sub-processor of any of the Relevant Terms to the extent required under Data Protection Law.

5.4 If the Services allow Customer to utilize its own vendors, including but not limited to third-party providers to extend the Services, unless otherwise expressly agreed in writing, such vendors are sub-processors of Customer and not Service Provider.

5.5 If Customer is a reseller of Service Provider ("Reseller"), Reseller shall enter into a data processing addendum with the end customer that complies with the Data Protection Laws.

6. SECURITY BREACH MANAGEMENT AND NOTIFICATION, DATA SUBJECT REQUESTS & FURTHER ASSISTANCE

6.1 Service Provider will notify Customer after awareness of any Security Breach that requires notification under Data Protection Law without undue delay, and for Personal Data under GDPR or UK GDPR within 48 hours after becoming aware of the Security Breach. Service Provider shall promptly and without undue delay investigate the Personal Data Breach, take reasonable steps to mitigate the effects of the Personal Data Breach to the extent within Service Provider's reasonable control, and provide Customer with all information required under Data Protection Laws. Service Provider's notification of or response to a Personal Data Breach under this Section 6.1 will not be construed as an acknowledgement by Service Provider of any fault or liability with respect to the Personal Data Breach. Notification(s) of a Security Breach, if any, will be delivered to one or more of Customer's business, technical or administrative contacts by any means Service Provider selects, including via email. It is Customer's sole responsibility to ensure it maintains accurate contact information on Service Provider's support systems at all times.

6.2 *Data Subject Requests.* To the extent legally permitted, Service Provider will promptly notify Customer if it receives a Data Subject Request. Service Provider will not respond to a Data Subject Request, provided that Customer agrees Service Provider may at its discretion respond to confirm that such request relates to Customer. Customer acknowledges and agrees that the Services may include features which will allow Customer or a Data Subject to manage Data Subject Requests directly through the Services without additional assistance from Service Provider. If Customer does not have the ability to address a Data Subject Request, Service Provider will, upon Customer's written request, provide reasonable assistance to facilitate Customer's response to the Data Subject Request to the extent such assistance is consistent with applicable law; provided that Customer will be responsible for paying for any costs incurred or fees charged by Service Provider for providing such assistance.

6.3 *Further Assistance.* Taking into account the nature of processing, the information available to Service Provider and the feasibility of the Customer request, Service Provider will provide such assistance as Customer reasonably requests in relation to Customer's obligations under Data Protection Laws with respect to (i) data protection impact assessments, (ii) notifications to the Supervisory Authority under Data Protection Laws and/or communications to data subjects by the Customer in response to a Security Breach, or (iii) Customer's compliance with its obligations under the GDPR or UK GDPR (as applicable) with respect to the security of processing. Customer will pay any costs or fees charged by Service Provider for providing the assistance in this Section 6.3.

7. AUDIT AND RECORDS

7.1 Service Provider shall make available to the Customer such information in Service Provider's possession or control as Customer may reasonably request with a view to demonstrating Service Provider's compliance with the obligations of data processors under Data Protection Law in relation to its processing of Personal Data. If available, Service Provider may fulfill an audit request via an independent third-party certification, audit or report against a recognized industry standard (such as SOC I or SOC 2). Except as expressly agreed otherwise in Service Provider's sole discretion, Customer acknowledges that due to the nature of the operations of Service Provider and its data center provider, on-site audits are not feasible; provided that solely to the extent required by applicable law, where the foregoing is insufficient to demonstrate Service Provider's compliance, at Customer's cost, after reasonable advance written notice, and not more than once per calendar year, Service Provider shall make efforts to offer any necessary information to comply with a commercially reasonable request in connection with an audit or inspection request.

8. CCPA

8.1 Where Customer is a "business" as defined and covered by the CCPA, or a service provider to such a business, the following section applies: Service Provider shall be a service provider to Customer under the CCPA, and to the extent required by the CCPA, Service Provider will not (i) sell or share (as such terms are defined in the CCPA) Personal Data; (ii) retain, use, or disclose Personal Data for any purpose other than for the specific purpose set forth in the Master Agreement of performing the Services, including retaining using or disclosing the Personal Data for a commercial purpose other than providing the Services, or as permitted by the CCPA; (iii) retain, use or disclose the Personal Data outside of the direct business relationship between Service Provider and Customer, unless expressly permitted by the CCPA; or (iv) combine the Personal Data that Service Provider receives in the Services with Personal Data that it receives from or on behalf of another person, or collects from its own interaction with the consumer, except as permitted by the CCPA. Each Party shall comply with the applicable sections of the CCPA. Each Party shall in connection with de-identified Personal Data comply with the terms concerning de-identified data in the CCPA. Service Provider shall notify Customer if it determines it can no longer meet its obligations under the CCPA. Customer may, upon written notice, take reasonable and appropriate stop and remediate Service Provider's unauthorized use of Personal Data, by suspending the provision of Personal Data from Customer to Service Provider. To the extent that other Data Protection Laws in the United States beyond the CCPA require the terms in this section to be set forth in a contract between a controller and processor, Service Provider shall also comply with the terms in this section for each such applicable Data Protection Law in the United States.

9. INTERNATIONAL DATA TRANSFERS

9.1 Customer agrees that its use of the Services will involve the transfer of Personal Data to, and processing of Personal Data in, locations outside of the UK, Switzerland and/or EEA from time to time, such as for purposes of providing support to Customer, including but not limited to processing in the United States.

9.2 **Transfers Pursuant to the Data Privacy Framework**

9.2.1 If the Service Provider self-certifies to EU-US Data Privacy Framework, the UK extension to the Data Privacy Framework [and the Swiss-US Data Privacy Framework] (collectively, "**Data Privacy Framework**"), any transfers of Personal data to the United States shall take place in accordance with the Data Privacy Framework.

9.3 **Transfers Pursuant to the Standard Contractual Clauses**

If the Data Privacy Framework is invalidated in whole or in part, or the Service Provider is not a participant in the Data Privacy Framework, then the Standard Contractual Clauses shall automatically apply instead of the Data Privacy Framework (or relevant part thereof) in accordance with this section 9.3.

9.3.1 *UK transfers:*

9.3.1.1 To the extent Personal Data is transferred to Service Provider and processed by or on behalf of Service Provider outside the UK (except if in an Adequate Country) in circumstances where such transfer would be prohibited by UK GDPR in the absence of a transfer mechanism, the parties agree that the EU Clauses subject to the UK Approved Addendum will apply. The UK Approved Addendum is incorporated into this Privacy Addendum.

9.3.1.2 Schedule 2 references the information required by Tables 1 to 4 inclusive of the UK Approved Addendum.

9.3.2 *EU transfers:*

9.3.2.1 To the extent Personal Data is transferred to Service Provider and processed by or on behalf of Service Provider outside the EEA (except if in an Adequate Country) in circumstances where such transfer would be prohibited by EU GDPR in the absence of a transfer mechanism, the parties agree that the EU Clauses will apply in respect of that processing and are incorporated into this Privacy Addendum in accordance with Schedule 4.

9.3.2.2 Schedule 4 contains the information required by the EU Clauses.

9.3.3 *Swiss transfers:*

9.3.3.1 To the extent Personal Data is transferred to Service Provider and processed by or on behalf of Service Provider outside Switzerland (except if in an Adequate Country) in circumstances where such transfer would be prohibited by Swiss Data Protection Laws in the absence of a transfer mechanism, the parties agree that the EU Clauses subject to the Swiss Addendum will apply in respect of that processing. The Swiss Addendum is incorporated into this Privacy Addendum.

9.3.3.2 Schedule 3 and Schedule 4 contains the information required for the Swiss Addendum, including for the purposes of transfers to which this section 9.3.3 applies.

9.3.4 Service Provider may (i) replace the EU Clauses, the Swiss Addendum and/or the UK Approved Addendum generally or in respect of the EEA, Switzerland and/or the UK (as appropriate) with any alternative or replacement transfer mechanism in compliance with applicable EU/UK Rules or applicable Swiss Data Protection Law, including any further or alternative standard contractual clauses approved from time to time and (ii) make reasonably necessary changes to this Privacy Addendum by notifying Customer of the new transfer mechanism or content of the new standard contractual clauses (provided their content is in compliance with the relevant decision or approval), as applicable.

10. GENERAL TERMS

10.1 Each party's and all of its affiliates' liability, taken together in the aggregate, arising out of or related to this Privacy Addendum whether in contract, tort or under any other theory of liability, is subject to the limitation of liability section of the Master Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its affiliates under the Master Agreement and this Privacy Addendum.

10.2 No alteration, amendment, or modification of this Privacy Addendum will be valid unless in writing and signed by an authorized representative of both parties.

10.3 Any ambiguity in the terms of this Privacy Addendum will be resolved to permit Service Provider and Customer to comply with the Data Protection Laws.

10.4 This Privacy Addendum is the entire and complete agreement between the parties with respect to the privacy and security of Personal Data and supersedes any other agreements, representations, or understandings whether oral or written. All clauses of the Master Agreement, that are not explicitly amended or supplemented by the clauses of this Privacy Addendum, and as long as this does not contradict with compulsory requirements of Data Protection Laws or other applicable laws, under this Privacy Addendum, remain in full force and effect and shall apply, including, but not limited to: Governing Law and Dispute Resolution, Jurisdiction, Limitation of Liability (to the maximum extent permitted by the Data Protection Laws and EU Clauses). If the Master Agreement does not contain a venue or jurisdiction for disputes and claims, Service Provider and Customer agree that, notwithstanding any language to the contrary, disputes between the Parties under the Standard Contractual Clauses may also be adjudicated in the United States to the extent not expressly prohibited by applicable laws.

10.5 Should any provision of this Privacy Addendum be found invalid or unenforceable pursuant to any applicable law, then the invalid or unenforceable provision will be deemed superseded by a valid, enforceable provision that most closely matches the intent of the original provision and the remainder of the Privacy Addendum will continue in effect.

10.6 If Customer engages Service Provider or its Affiliate in paid professional services, the Customer shall expressly set forth any data protection requirements for the project in writing in the statement of work or quote ("Order") for such services. The Order shall identify any processing of Personal Data required of Service Provider under this Privacy Addendum. In the event no data protection requirements and processing is set forth in the Order, then this DPA does not apply to the professional services.

10.7 Service Provider may update this Privacy Addendum from time to time, with such updated version posted to https://khoros.com/legal/customer-agreementsor a successor website designated by Service Provider with an email or other notification to Customer; provided, however, that no such update shall materially diminish the privacy or security of the Personal Data.

10.8 The Privacy Addendum does not benefit or create any right or cause of action on behalf of any third party, but without prejudice to the rights or remedies available to Data Subjects under Data Protection Laws or the SCCs.

10.9 If Service Provider makes a determination that it can no longer meet its obligations in accordance with this Privacy Addendum, it shall promptly notify the Customer of that determination, and cease the processing or take other reasonable and appropriate steps to remediate.

10.10 Notices required under this Privacy Addendum shall be sent according to the Master Agreement with a copy (which shall not constitute notice) to both the usual point of contact or support at Service Provider and via e-mail to: privacy@khoros.com.

SCHEDULE 1

Data Processing Details

For the purposes of the Privacy Addendum and Schedules 2. 3 and 4, the parties set out below a description of the Personal Data being processed under the Master Agreement and further details required pursuant to the EU/UK Rules.

Subject Matter of the Processing	Service Provider's provision of the Services to Customer.
Nature and purpose of Processing	The collection and storage of Personal Data pursuant to providing the Services to Customer.

Types of Personal Data	Personal Data that Customer in its discretion uploads into the Services or Service Provider is directed to collect. Khoros Communities- Khoros uses online Personal Data such as user ID, user name, and email address. Optionally, users can provide additional information such as location, title, and IM screen names. Khoros Marketing and Khoros Care - Khoros processes public data from social media networks such as user handle, public tweets, public posts. Khoros may Process direct messages between the data exporter representatives using the services and the end users of data exporter on various social media networks. Additionally, Khoros processes data exporter's employee data such as user ID, user name, and email address for log-in purposes and when employee makes notes within the Khoros platform. Khoros may also use this personal contact information to communicate with users on or off the platform for subscription notices or account updates. Khoros Bot- Khoros Processes direct messages between the data exporter representatives using the services and the end users of data exporter on various social media networks and messaging channels. Additionally, Khoros may Process data exporter's employee data such as user ID, user name, and email address when employee uses the Khoros platform. Khoros may also use this personal contact information to communicate with users on or off the platform for subscription notices or account updates. All Products- Khoros tracks usage of Khoros products and provides reporting and usage metrics to Khoros customers (the data exporters). Khoros collects some personal information indirectly such as the browser User-Agent header, IP address, HTTP referrer header, and the request URL. This information is used to provide a personalized experience for the end user (data subject) and for reporting purposes to make our product and services better.
Sensitive Personal Data and applied restrictions	None

Categories of Data Subject	Data Subjects may include any end users or others (including without limitation employees, customers, or suppliers) about whom Personal Data is provided to Service Provider via the Services by, or at the direction of, Customer.
Duration of Processing	For the duration of the Master Agreement, or until the processing is no longer necessary for the purposes.

SCHEDULE 2

UK transfers

For the purposes of the UK Approved Addendum,

1. the information required for Table 1 is contained in Schedule 1 of this Privacy Addendum and the start date shall be deemed dated the same date as the EU Clauses;
2. in relation to Table 2, the version of the EU Clauses to which the UK Approved Addendum applies is Module Two for Controller to Processor and Module Three for Processor to Processor transfers (as applicable);
3. in relation to Table 3, the list of parties and description of the transfer are as set out in Annex I of Schedule 4 of this Privacy Addendum, Service Provider's technical and organisational measures are set in section 4.1 of this Privacy Addendum, and the list of Service Provider's sub-processors shall be provided pursuant to section 5.2 of this Privacy Addendum; and
4. in relation to Table 4, neither party will be entitled to terminate the UK Approved Addendum in accordance with clause 19 of the UK Mandatory Clauses.

SCHEDULE 3

Swiss Addendum

In respect of transfers otherwise prohibited by Swiss Personal Data:

1. The FDPIC will be the competent supervisory authority;

2. Data subjects in Switzerland may enforce their rights in Switzerland under Clause 18c of the EU Clauses, and

3. References in the EU Clauses to the GDPR should be understood as references to Swiss Data Protection Law insofar as the data transfers are subject to Swiss Data Protection Law.

SCHEDULE 4

EU Clauses

1. For the purposes of this Schedule 4, the EU Clauses (Module II and Module III as applicable), available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN, shall be incorporated by reference to this Schedule and the Privacy Addendum and shall be considered an integral part thereof, and the Parties' signatures in the Privacy Addendum, or Master Agreement (as applicable) shall be construed as the Parties' signature to the EU Clauses. In the event of an inconsistency between the Privacy Addendum and the EU Clauses, the latter will prevail.

2. For the purposes of the EU Clauses, the following shall apply:

   - Customer shall be the data exporter and Service Provider shall be the data importer. Each Party agrees to be bound by and comply with its obligations in its role as exporter and importer respectively as set out in the EU Clauses.

   - Clause 7 (Docking clause) shall be deemed as included.

   - Clause 9 (Use of sub-processors): OPTION 2 – GENERAL WRITTEN AUTHORISATION shall apply. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors as set out in clause 4 of the Privacy Addendum.

   - Clause 11 (Redress): optional clause (optional redress mechanism before an independent dispute resolution body) shall be deemed as not included.

   - Clause 13 (a) (Supervision):

     - *[Where Customer is established in an EU Member State*:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

     - [*Where Customer is not established in an EU Member State but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:*] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority. [OR]

     - [*Where Customer is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679*:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

   - Clause 17 (Governing law):

     These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

   - Clause 18 (b) (Choice of forum and jurisdiction): The Parties agree that any dispute between them arising from the EU Clauses shall be resolved by the courts of Ireland.

3. To the extent not prohibited by applicable law, any provision in the EU Clauses relating to liability of the parties with respect to each other shall be subject to the limitations and exclusions of the Master Agreement.

4. Any provision in the EU Clauses relating to the right to audit shall be interpreted in accordance with the Master Agreement and section 7 of the Privacy Addendum.

ANNEX I to Schedule 4

A. LIST OF PARTIES

Data exporter(s):
Name: Customer as specified on the Quote
Address: As specified on the Quote
Contact person's name, position and contact details: As specified on the Quote or available on Customer's Privacy Policy
Activities relevant to the data transferred under these Clauses: data exporter will transfer Personal Data to the data importer as required for the provision of Services by the data importer under the Master Agreement and as set out in the Privacy Addendum.
Signature and date: please refer to signature and date in the Privacy Addendum or Master Agreement.
Role (controller/processor): Controller or Processor, as appropriate

Data importer(s):
Name: Service Provider as specified on the Quote
Address: As specified on the Quote
Contact person's name, position and contact details: Available on Privacy Policy.
Activities relevant to the data transferred under these Clauses: data importer will process personal data as required for the provision of Services under the Master Agreement and as set out in the Master Agreement.
Signature and date: signature and date in the Privacy Addendum or Master Agreement.
Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred
See Schedule I to the Privacy Addendum

Categories of personal data transferred
See Schedule I to the Privacy Addendum

Sensitive data transferred (if applicable) and applied restrictions or safeguards
See Schedule I to the Privacy Addendum

Frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).
Transfers will occur from time to time as required during the course of the performance of the Services under the Master Agreement.

Nature of the processing
See Schedule 1 to the Privacy Addendum

Purpose(s) of the data transfer and further processing
See Schedule 1 to the Privacy Addendum

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
See Schedule 1 to the Privacy Addendum

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing
Available on request in accordance with section 4.2 of the Privacy Addendum

C. COMPETENT SUPERVISORY AUTHORITY
Identify the competent supervisory authority/ies in accordance with Clause 13

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL FOR THE SECURITY OF THE PERSONAL DATA
See section 4 of the Privacy Addendum

ANNEX III – LIST OF SUB-PROCESSORS
Available at https://khoros.com/khoros-subprocessors

SCHEDULE 5

Security Measures

Data Importer will implement technical and organizational measures for the protection of the security, confidentiality and integrity of Personal Data with respect to the services or other obligations with the contracting party ("Customer") and/or the Data Exporter (as applicable, where Data Exporter is not the Customer), including the following measures:

1. Physical Security – Maintain hosting at a secure facility (such as AWS) with data center access restrictions, monitoring, security staff, and other physical security measures.

2. System and Network Security – Maintain network access restrictions, firewalls, server hardening measures, and user authentication protocols designed to protect the security of Personal Data.

3. Information Security Policy – Maintain a written information security policy with measures designed to (i) provide for the security and confidentiality of Personal Data; (ii) protect against anticipated threats or hazards to the security of the Personal Data; and (iii) protect against unauthorized access or use of Personal Data in ways that could result in substantial harm to Customer or Data Importer.

4. Security Incident Management – Maintain information security incident management procedures regarding the internal reporting, investigation, and mitigation of security incidents. Report a Personal Data Breach to Customer in accordance with applicable laws.

5. Risk Management –Conduct risk assessments on a periodic basis to identify and mitigate risks to Personal Data. Perform web application scans and/or training based on the Open Web Application Security Project (OWASP) Top 10. Periodically review and test the information security safeguards.

6. Encryption – Encrypt Personal Data where feasible and commercially reasonable in accordance with industry standards for encryption at rest and in transit.

7. Business Continuity; Backups – Establish and maintain standards, processes and controls for the timely recoverability of business critical data and information processing systems. Maintain periodic backups and archive methodologies in accordance with the practices of Data Importer and the agreement with Customer. Ensure data centers have redundant power, provisions against fire and natural disasters, and other measures to ensure the reliability of services.

8. Staff Management – Ensure the workforce has agreed in writing to maintain the confidentiality of Personal Data and is aware of the obligations under privacy and/or security laws concerning Personal Data through annual training. Conduct background checks on applicants for employment and consulting projects in accordance with applicable law.

9. Account Identification, Authorization and Access – Use and access to Personal Data is limited to the purposes of the services or otherwise as agreed with the Customer. Access of team members is granted on the principle of least privilege on a role basis and subject to authorization and deactivation practices of Data Importer. Access is subject to password restrictions and other user management and authentication practices designed to ensure the security of accounts. Personal Data is subject to physical or logical segregation from the Personal Data of other customers.

10. Event Logging – Maintain event logging in accordance with the agreement with Customer and the practices of Data Importer.

11. Data Minimization – Create and/or collect Personal Data as necessary for the services and as agreed with, or to the extent processing on behalf of Customer instructed by, Customer.

12. Data Subject Access Rights (DSAR) - Maintain appropriate processes to enable and/or facilitate the fulfilment of DSAR requests.

13. Data Retention – Maintain Personal Data in accordance with the agreement with Customer and, where a processor, the instructions of Customer. Return or destroy Personal Data in accordance with applicable law, the agreement with Customer and the practices of Data Importer. Maintain appropriate security measures and procedures to destroy removable media containing Personal Data, or alternatively, to render Personal Data on such media unintelligible and not capable of reconstruction.

14. Subprocessors – Enter into contractual commitments with its subprocessors as necessary and/or required by applicable law. Subprocessors may offer different, but not less protective, technical and organizational measures.

15. Changes – Data Importer may change the technical and organizational measures in effect from time to time, in its sole but reasonable discretion, so long as it does not materially reduce the overall level of privacy and security protection offered by the technical and organizational measures.