Revised: August 19, 2024

TO BE DELETED ONCE CONTRACT NEGOTIATED

KHOROS MASTER SERVICE AGREEMENT GUIDE: WHAT IS KHOROS?

Khoros is a Digital Engagement Platform: Khoros is a software as a service company that offers you a one-stop platform on which to digitally engage with your customers. You can also connect other software to our platform to provide a complete picture of your customer journey and engagement – be it for social media management or your digital contact center.

Products On Our Platform

Khoros Community: An interactive space for individuals to congregate, collaborate, and create content about your brand. Communities provide brand-to-customer engagement and allow for peer-to-peer self-service, recommendations, and shared experiences.
Khoros Marketing: Simplify your Khoros Marketing operations and campaigns to centrally manage (plan, publish, and optimize) your social media accounts and export social media data with configurable analytics.
Khoros Care: Engage with your customers across all channels through a central hub across a variety of digital engagement channels (in-app messaging, SMS, Social Media Networks, email, etc.), scaling outbound digital communications with automation. You can prioritize, tag, filter, and route inbound communications into a single queue for your agents.
Khoros Bot: Utilize an AI-powered, natural-language chat bot to engage your customers with proactive, personalized automated services to reduce customer effort and service costs.

Support Services

Professional Services: Our professional services ("Professional Services") team goes beyond simple platform enablement and initial deployment by ensuring you are getting the most out of our partnership through continued account management, technical assistance, integrations, and third-party collaborations.
Strategic Services: Our strategic services ("Strategic Services") team helps you develop and execute strategic marketing and/or campaign plans, overarching brand and digital presence strategy, and digital engagement management and moderation.

Data Protection Information

Data Ownership: You own the data and content ingested into the Khoros platform and any Strategic Services. We own all IP rights to the platform, our Professional Services, and the backend data derived concerning platform use and performance.
Consent & Security: You are responsible for obtaining consents from your end users to process their personal data. When we receive data from you, we process that data and rely on your consents. In turn, we secure that data in our platform according to ISO 270001 and similar standards. We also engage independent auditors to conduct an annual SSAE 18 SOC 2 audit.
Personal Data Inventory: The data we process contains personally identifiable information. You can find a breakdown of the personal data each product collects here. This inventory includes each data element, the source of the data, subprocessor recipient(s), and the specific retention period.
Subprocessors: We use certain subprocessors when we provide our services to you. You can find the information that you need about our subprocessors here.
Retention, Export, Deletion:

Product	Retention	Export
Khoros Community	Duration of contract	Upon request and sent by Khoros to you within 30 days of expiration/termination of contract.
Khoros Care	Duration of contract, but data ingested from certain social media platforms may only be retained for a rolling 18-month period.	Available for self-service export via API.
Khoros Marketing	Duration of the contract, but data ingested from certain social media platforms may only be retained for a rolling 24-month period.	Available for self-service export via API.
Khoros Bot	Duration of contract	Available for self-service export via API.

We retain your data in accordance with our data retention and deletion policy here, and will also delete your data 30 days after our contract ends, except for the following: (1) as required by applicable law; (2) we maintain backup data for 90 days for business continuity practices; and/or (3) we maintain log files for up to 12 months for security reasons.

KHOROS MASTER SERVICE AGREEMENT

This Master Service Agreement ("MSA") is between Khoros, LLC, and its subsidiaries ("Khoros") and Customer (as named in the signature block). The MSA's "Effective Date" is the date of the last signature on this MSA.

1. KHOROS'S RESPONSIBILITIES TO CUSTOMER

1.1 **Provide Services to Customer.** Khoros will provide: (a) access to and use of its software-as-a-service platform and applications, which includes documentation and developer documentation (collectively, "Documentation"), user interface, associated tools, and programming (together known as the "Subscription Services"), to Customer and its Authorized Users in accordance with the applicable service order ("SO"); and, if applicable, (b) all strategic services, enablement, configuration, customization, integration, data import, export, extraction, monitoring, technical assistance, maintenance, training, or other services ("Professional Services") detailed in a Statement of Work ("SOW"). This MSA refers to Subscription Services and Professional Services together as "Services." "Authorized User(s)" means Customer's employees, contractors, and/or authorized agents.

1.2 **Allow Approved Affiliates to Obtain Services Under This MSA.** If an Affiliate (as defined below) signs a SO/SOW that references this MSA, then the term "Customer" in this MSA refers to the Affiliate signing the SO/SOW. If an Affiliate uses Services provided under an SO/SOW but does not sign the SO and/or is not referenced in the SO, Customer is jointly and severally liable for the acts or omissions of that Affiliate. An "Affiliate" is an entity owned or controlled by Customer or under common ownership with Customer that is not located in a country subject to a US embargo or has data localization requirements as defined in Section 4.2. "Control" means that Customer has more than 50% voting interest in the Affiliate.

1.3 **Meet Service Level Commitments.** Khoros provides its Subscription Services according to its Service Level Agreement ("SLA") (https://khoros.com/service-level-agreement), which is incorporated herein by reference. The remedies provided within the SLA are the sole remedies for SLA issues. SLA issues are not material breaches of this MSA.

1.4 **Keep Subscription Services Updated.** Khoros continually improves and refines its Subscription Services to support or enhance the quality, performance, and/or security of its Subscription Services. Except for changes due to the Social Media Networks (as defined below) and as set forth in Section 7.4, Khoros's changes will not materially degrade the performance of the Subscription Services. Notwithstanding the foregoing, if Khoros or any of its licensors materially changes or ceases offering any material element of the Services, Khoros may effect such change or cessation following reasonable notice to Customer. Except as required by applicable law, Khoros will not be obligated to refund any amounts paid for the Services if Khoros changes or ceases to offer any material element of the Services in accordance with this Section.

1.5 **Connect Certain Third-Party Applications.** Khoros permits Customer to connect third-party applications that are not owned by Khoros ("Third-Party Applications") to certain Subscription Services. Before connecting a Third-Party Application, Customer must obtain written approval from Khoros. Some Third-Party Applications require Customer to enter into a separate agreement with the Third-Party Application before the Third-Party Application can be connected to the Subscription Services. If Customer chooses to connect a Third-Party Application to the Subscription Services, any issue concerning or caused by the Third-Party Application is not a material breach under this MSA or SO. Finally, to maintain the security, operability, and performance of the Subscription Services, Khoros may control how much data a Third-Party Application requests and/or retrieves from the Subscription Services; provided, however, that Khoros will provide notice to Customer to the extent reasonably practicable prior to controlling the amount of data requested and/or retrieved from the Subscription Services.

1.6 **Comply with All Applicable Laws.** Khoros will comply with all laws applicable to Khoros, including, without limitation, laws governing the protection of personally identifiable information and other laws applicable to data protection and privacy.

2. CUSTOMER'S RESPONSIBILITIES TO KHOROS

2.1 **Customer Is Responsible for Its Authorized Users.** Customer is responsible for: (a) the actions and omissions of its Authorized Users' use of the Subscription Services; (b) ensuring that its Authorized Users secure their access and passwords to the Subscription Services; and (c) using the Subscription Services in accordance with the Documentation. Authorized User credentials cannot be shared or used by more than one person (but may be reassigned, in its entirety). For its Authorized Users, Customer shall notify Khoros immediately of any known or suspected phishing attempt, password compromise, and/or breach of security, and shall use best efforts to stop said issues.

2.2 **Customer Will Comply with Social Media Network Terms.** When a Social Media Network is connected to the Subscription Service, Customer will comply with the terms of service and/or use of a Social Media Network. "Social Media Network" means social media providers such as X (f/k/a Twitter), Facebook, Instagram, Google, WhatsApp, and other providers or websites that solicit content from users, make such content available for resyndication or publication via their application programming interface ("API"), and are used by Customer through the Subscription Services. Khoros does not control the operability or features of the Social Media Networks and/or the content posted by third parties to a Social Media Network ("Social Media Content").

2.3 **Customer Agrees to Abide by Usage Limits.** Each SO defines the Customer's specific usage rights and/or limits for the Subscription Services. If Khoros: (a) determines that Customer has exceeded its usage rights or limits; (b) notifies Customer about the overuse; and (c) gives Customer 5 days to cure the overuse and Customer fails to do so, Customer agrees to pay Khoros additional fees for such unauthorized and/or additional usage at the then current list price (without the need for the parties to amend the SO).

2.4 **Customer Shall Not Misappropriate the Services.** Customer shall not (and shall not allow a third-party to): (a) copy or republish, reverse engineer, decompile, disassemble, or otherwise try to derive or copy the source code of the Subscription Services or its features and tools for any reason; or (b) engage in any web scraping, API scraping, or data scraping of the Subscription Services.

2.5 **Comply with All Applicable Laws.** Customer will comply with all laws applicable to Customer, including, without limitation, laws governing the protection of personally identifiable information and other laws applicable to data protection and privacy. This includes, but is not limited to, obtaining required consent, providing required privacy notices, and taking reasonable steps to prevent and discourage users from providing Sensitive Personal Information (as defined below).

3. THE PARTIES' INTELLECTUAL PROPERTY RIGHTS

3.1 **Khoros Intellectual Property Rights.** Khoros owns and retains right, title, and interest to the Services, and any modifications, improvements, or enhancements to the Services. Khoros also owns and retains right, title and interest to Usage Data. Customer has no intellectual property license or rights to the Services or Usage Data. Customer recognizes that the Services and Usage Data are protected as or by trade secrets, copyrights, patents, and/or other laws. "Usage Data" is data from the Khoros backend system concerning the use and performance of the Services.

3.2 **Khoros Owns Feedback About the Services.** Khoros owns any Feedback Customer provides about the Services. As such, Khoros may use, profit from, disclose, publish, keep secret, or otherwise exploit the Feedback, without compensating or crediting Customer, the Authorized User, or end user in question. "Feedback" is any suggestion or idea for improving, enhancing, and/or modifying the Services.

3.3 **Customer Intellectual Property Rights.** Customer owns and retains right, title, and interest to: (a) Customer Data; and (b) any Professional Services developed specifically and exclusively for Customer under a SOW. "Customer Data" means data in electronic form or information submitted by Customer, Customer's Authorized Users, and/or by Customer's customers/end users. Customer Data also includes any Customer-provided software, logos, or other Customer-owned materials inserted or added to the Subscription Services (e.g., headers, footers, sidebars, graphics).

3.4 **Khoros's Use of Customer Data.** Customer authorizes Khoros to access, process, and use Customer Data and to share Customer Data with Khoros's subprocessors and Third-Party Applications, as is necessary to provide the Services.

4. DATA PROTECTION & SECURITY

4.1 **Data Protection.** The parties agree to the Data Protection Agreement ("DPA") attached as Exhibit A.

4.2 **Data Localization.** Customer shall not knowingly allow Authorized Users to be located in or market to end-users located in jurisdictions that require data localization to access or use the Services.

4.3 **Security.** During the MSA's Term (as defined below) Khoros will: (a) maintain an information security program that requires administrative, technical, and physical safeguards relating to its Subscription Services platform to protect Customer Data; (b) maintain AICPA SOC 2 Type 2 and ISO compliance certification; and (c) maintain technical and organizational measures to ensure a level of security appropriate for the Services. In the event Khoros is directly involved in the processing, storage, or transmission of payment cardholder data as a part of the Services, Khoros will comply with the applicable service provider requirements of the Payment Card Industry Data Security Standards ("PCI DSS").

4.4 **No Sensitive Personal Information**. Customer will not use the Services to process (or use the Services to collect) any Sensitive Personal Information unless its processing is expressly supported as a feature of the applicable Service in the applicable Documentation. Khoros shall have no liability under this Agreement for Sensitive Personal Information submitted in violation of the foregoing. "Sensitive Personal Information" means (i) special categories of personal data enumerated in European Union Regulation 2016/679, Article 9(1) or any successor legislation; (ii) patient, medical, or other protected health information regulated by the Health Insurance Portability and Accountability Act, as amended and supplemented ("HIPAA"); (iii) credit, debit or other payment card data subject to PCI DSS; (iv) other personal information subject to regulation or protection under specific laws such as the Gramm-Leach-Bliley Act (or related rules or regulations); (v) social security numbers, driver's license numbers, or other government ID numbers; or (vi) any data similar to the foregoing that is protected under applicable laws or regulations.

5. CONFIDENTIAL INFORMATION

5.1. **Confidential Information Definition.** "Confidential Information" is: (a) non-public Customer Data; (b) any document the disclosing party marks "Confidential;" (c) the Services documentation (including developer documents); and (d) any other nonpublic, sensitive information the receiving party should reasonably consider a trade secret or otherwise confidential (e.g., this MSA, SOs, SOWs, pricing information, Services functionality, and product roadmaps). Confidential Information does not include information that: (i) is in the receiving party's possession at the time of disclosure without obligations of confidentiality; (ii) is independently developed by the receiving party without use of or reference to Confidential Information; (iii) is or becomes known or disclosed publicly, before or after disclosure to the receiving party, other than as a result of the receiving party's improper action or inaction; or (iv) is approved for release in writing by the disclosing party.

5.2 **Retention of Rights.** Each party retains right, title, and interest to all its Confidential Information. The parties do not transfer ownership of Confidential Information or grant a license to such information unless specified in this MSA.

5.3 **Nondisclosure & Non-Use.** Each party shall only use the other party's Confidential Information in connection with the Services. The receiving party: (a) shall not disclose Confidential Information to any employee or contractor of the receiving party unless such person needs access to such information as part of their job and is bound to this confidentiality clause; and (b) except as noted in Section 3.4, shall not disclose Confidential Information to any other third party without the disclosing party's prior, written consent. Further, the receiving party shall protect Confidential Information with the same degree of care it uses to protect its own Confidential Information of similar nature and importance, but with no less than reasonable care. The receiving party shall promptly notify the disclosing party of any misuse or misappropriation of Confidential Information that comes to the receiving party's attention. However, the receiving party may disclose Confidential Information if required by law or governmental authority. The receiving party shall give the disclosing party prompt notice (if legally permissible) of any such demand and reasonably cooperate with the disclosing party, at the disclosing party's expense, in any effort to seek a protective order or otherwise to contest such required disclosure.

5.4 **Exception to Confidentiality of This MSA.** This MSA and its SOs/SOWs may be disclosed in confidence to legal counsel or professional advisors who need to know in the context of a merger, financing, audit, or similar transaction.

5.5 **Injunction.** The parties agree that breach of this confidentiality section may cause irreparable injury, for which monetary damages would be inadequate compensation, and that, in addition to any other remedy, the disclosing party may seek injunctive relief against the breach or threatened breach without proving actual damage or posting a bond/security.

6. PAYMENT & SERVICE CREDITS

6.1 **Fees.** Customer shall pay Khoros the fees provided in each SO (the "Subscription Fee") and/or fees in each SOW ("Professional Services Fee"). The Subscription Fee and Professional Services Fee are referred to together herein as the "Fee(s)." To the extent applicable, Fees shall also include, but are not limited to, any fees relating to Customer's use of Social Media Networks as part of the Services, which may be charged as a separate line item in Customer's SO. Khoros's invoices are payable 30 days from the date on the invoice. Khoros is not required to refund the Subscription Fee, in whole or in part, unless specifically noted in this MSA.

6.2 **Expenses.** Customer will reimburse Khoros for its reasonable out-of-pocket travel and related expenses incurred in performing the Services. Khoros will notify Customer and obtain Customer's written pre-approval prior to incurring such expenses.

6.3 **Payment Disputes.** If Customer disputes the accuracy of any Fees or expenses contained in an invoice, Customer must provide Khoros with notice of the disputed amount with reasons for the dispute within 30 days after receiving the invoice. If Customer only disputes a portion of an invoice, the undisputed amount is payable to Khoros on time, as defined in Section 6.1. Non-payment of undisputed Fees is a material breach of this MSA.

6.4 **Taxes.** Customer shall pay and be liable for all taxes relating to Khoros's provision of Services. Khoros shall pay and be liable for taxes based on its net income or capital.

6.5 **Customer Purchase Orders.** If Customer requires an internal purchase order to pay Fees, Customer agrees that it will issue a purchase order within enough time to meet its payment obligations to Khoros outlined in Section 6.1.

6.6 **Service Credits.** If Khoros issues service credits under the SLA or as goodwill, those credits apply only towards outstanding or future invoices and are forfeited upon MSA termination.

7. REPRESENTATIONS, WARRANTIES & DISCLAIMERS

7.1 **Representations & Warranties Made by Khoros to Customer.** Khoros represents and warrants that: (a) it owns the Services, or has a valid license for same, and that it has and will maintain the ability to provide the Services; (b) the Services will materially conform to the specifications noted in Khoros's documentation about the Services; and (c) Professional Services will be performed according to industry standards. For Subscription Services, if Khoros breaches any of these warranties, Khoros shall, at its own expense: (i) secure for Customer the right to continue using the Services; (ii) replace or modify the Services to make them non-infringing; (iii) terminate the infringing features of the Services and refund to Customer any prepaid Fees for such features, proportional to the term left after such termination; and/or (iv) modify the Services to ensure its substantial conformance. For Professional Services, if Khoros breaches any of these warranties, Khoros shall, at its own expense, work in good faith with Customer to correct and improve the performance. In conjunction with Customer's indemnity rights, this is Khoros's sole obligation and liability, and Customer's sole remedy, for breach of these warranties. These representations and warranties do not apply to use of the Services in combination with hardware or software not provided by Khoros.

7.2 **Representations & Warranties Made by Customer to Khoros.** Customer represents and warrants that: (a) it has read and has the full right and authority to enter into, execute, and perform its obligations under this MSA; (b) it has obtained or will obtain all necessary consents of its Authorized Users and customers/end-users to process any personal data under this MSA; (c) it has not knowingly provided any inaccurate information about itself to Khoros or through the Services; and (d) it uses anti-virus protection on any Customer-owned devices that will access the Services.

7.3 **WARRANTY DISCLAIMERS.** THE WARRANTIES IN SECTION 7.1 & SECTION 7.2 ARE THE ONLY WARRANTIES MADE BY THE PARTIES. THE PARTIES MAKE NO OTHER WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR ANY IMPLIED WARRANTY ARISING FROM STATUTE, COURSE OF DEALING, COURSE OF PERFORMANCE, OR USAGE OF TRADE.

7.4 **SOCIAL MEDIA NETWORK DISCLAIMER.** CUSTOMER ACKNOWLEDGES THAT APPLICATION FEATURES THAT INTEROPERATE WITH SOCIAL MEDIA NETWORKS DEPEND ON THE CONTINUING AVAILABILITY OF THOSE SOCIAL

MEDIA NETWORKS' API AND PROGRAM. IF ANY SOCIAL MEDIA NETWORK STOPS PROVIDING ACCESS TO SOME OR ALL OF THE FEATURES OR FUNCTIONALITY CURRENTLY OR HISTORICALLY AVAILABLE TO KHOROS, OR STOPS PROVIDING ACCESS TO SUCH FEATURES OR FUNCTIONALITY ON REASONABLE TERMS, AS DETERMINED BY KHOROS IN ITS SOLE DISCRETION, KHOROS RESERVES THE RIGHT TO STOP PROVIDING ACCESS TO SUCH SOCIAL MEDIA NETWORK'S FEATURES OR FUNCTIONALITY AS PART OF THE SERVICES. KHOROS WILL NOT BE LIABLE TO CUSTOMER FOR ANY REFUNDS OR ANY DAMAGE OR LOSS OR ARISING FROM, OR IN CONNECTION WITH, ANY CHANGE MADE BY THE SOCIAL MEDIA NETWORK OR ANY RESULTING CHANGE TO THE SERVICES. CUSTOMER IRREVOCABLY WAIVES ANY CLAIM AGAINST KHOROS WITH RESPECT TO ANY SUCH CHANGE TO THE SERVICES.

8. INDEMNIFICATION

8.1 **Khoros Obligations to Indemnify Customer.** Khoros shall defend, indemnify, and hold harmless Customer and Customer Associates (as defined below) against any third-party claim, suit, or proceeding alleging that: (a) Khoros has breached this MSA or DPA; and/or (b) the Services infringe any intellectual property rights of a third party. Khoros's indemnification obligation does not apply to portions of the Services: (i) not provided by Khoros; (ii) made in whole or part in accordance with Customer's modifications; or (iii) where Customer's use of the Services is not in accordance with this MSA, DPA, or related SO/SOW. "Customer Associates" are Customer's officers, managers, directors, shareholders, parents, subsidiaries, agents, employees, contractors, successors, and assigns.

8.2 **Customer Obligations to Indemnify Khoros.** Customer shall defend, indemnify, and hold harmless Khoros and Khoros Associates (as defined below) against any third party claim, suit, or proceeding alleging that: (a) Customer breached this MSA or DPA; (b) infringement claims related to Customer's use of Social Media Content and/or Customer Data; and (c) claims that use of the Services through Customer's account harasses, defames, defrauds, unlawfully surveils a third party, or violates any law or restriction applicable to Customer on electronic advertising. Customer's indemnification obligation does not apply to the extent the indemnification claim is related to Khoros's breach of this MSA or DPA. "Khoros Associates" are Khoros's officers, managers, directors, shareholders, parents, subsidiaries, agents, employees, contractors, successors, and assigns.

8.3 **Indemnification Procedure.** These indemnification obligations are subject to the following conditions: (a) prompt written notice from one party to the other; (b) complete control of the defense and settlement by the indemnifying party (provided that the indemnifying party may not settle any claim without the indemnified party's consent, which may not be unreasonably withheld); and (c) reasonable cooperation by the indemnified party. The indemnifying party's obligations in this section include retention and payment of attorneys and payment of court costs, as well as settlement at indemnifying party's expense and payment of judgments. The indemnified party will have the right, not to be exercised unreasonably, to reject any settlement or compromise that requires it to admit wrongdoing or liability or subjects it to any ongoing affirmative obligations.

8.4. **Exclusive Remedy.** This Section 8 provides the indemnifying party's sole liability to and the indemnified party's exclusive remedy against the other party for any claims described in this Section.

9. LIABILITY, DAMAGES, CAPS, & EXCLUSIONS

9.1 **Mutual Liability Cap for Direct Damages.** EXCEPT FOR LIABILITY FOR BREACH OF: SECTION 3.1 (KHOROS INTELLECTUAL PROPERTY RIGHTS); SECTION 4 (DATA PROTECTION & SECURITY); SECTION 5 (CONFIDENTIAL INFORMATION); SECTION 6 (PAYMENT & SERVICE CREDITS); AND SECTION 8 (INDEMNIFICATION), NEITHER PARTY'S CUMULATIVE LIABILITY FOR DIRECT DAMAGES FOR ALL CLAIMS ARISING OUT OF OR RELATED TO THIS MSA SHALL EXCEED THE AMOUNT PAID OR PAYABLE BY THE CUSTOMER FOR THE SERVICE IMPLICATED DURING THE 12 MONTHS PRIOR TO THE EVENT THAT TRIGGERS LIABILITY.

9.2 **Exclusion of Indirect Damages.** EXCEPT FOR A PARTY'S VIOLATION OR INFRINGEMENT OF THE OTHER PARTY'S OR A THIRD-PARTY'S INTELLECTUAL PROPERTY RIGHTS, TO THE EXTENT PERMISSIBLE BY LAW, NEITHER PARTY SHALL BE LIABLE FOR LOST PROFITS OR LOSS OF BUSINESS OR FOR ANY CONSEQUENTIAL, INDIRECT, SPECIAL, INCIDENTAL, OR PUNITIVE DAMAGES.

9.3 **Exclusion of Liability & All Damages.** KHOROS DISCLAIMS ANY LIABILITY AND RESPONSIBILITY FOR DAMAGES RELATED TO: (A) THIRD-PARTY APPLICATIONS; (B) STOLEN, LOST, OR PHISHED PASSWORDS OF

CUSTOMER'S AUTHORIZED USERS OR FROM ANY SECURITY BREACHES THAT RESULT FROM CUSTOMER'S ACTION OR OMISSIONS WITH RESPECT TO SYSTEMS AND PROCESSES CONTROLLED BY CUSTOMER; AND (C) SOCIAL MEDIA NETWORKS AND/OR SOCIAL MEDIA CONTENT.

9.4 **Clarifications.** THE LIABILITIES LIMITED IN THIS SECTION APPLY: (A) TO LIABILITY FOR NEGLIGENCE; (B) REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT, STRICT PRODUCT LIABILITY, OR OTHERWISE; AND (C) EVEN IF A PARTY IS ADVISED IN ADVANCE OF THE POSSIBILITY OF THE DAMAGES IN QUESTION AND EVEN IF SUCH DAMAGES WERE FORESEEABLE.

10. TERM, SUSPENSION, & TERMINATION

10.1 **Term.** The MSA's term (the "Term") begins on the Effective Date and continues for the period noted in each SO/SOW under this MSA.

10.2 **Suspension.** Khoros may temporarily suspend the Services: (a) without notice, if Khoros reasonably concludes that Customer or another third-party's access to or use of the Services is causing immediate and ongoing harm to Khoros, Customer, or others (in this extraordinary case, Khoros agrees to immediately notify Customer of such suspension and use its best efforts to work with Customer to resolve the issue); or (b) with 10 days' notice, if Customer fails to timely pay Khoros for undisputed Fees. Khoros shall not be liable to Customer or to any third party for any liabilities, claims, or expenses arising from or related to such suspension.

10.3 **Termination for Material Breach.** Either party may terminate the MSA, SO, or SOW for material breach by providing written notice to the other party detailing the date and nature of the material breach. Termination will be effective 30 days after the notice is sent unless the other party cures the material breach before the 30 days has run. If Khoros terminates this MSA, or an SO or SOW for material breach, then Customer shall pay Khoros, within 30 days of termination, all remaining Fees due under this MSA, SO, and/or SOW, as applicable. If Customer terminates this MSA, a SO, or a SOW for material breach, Khoros shall refund Customer all unused, pre-paid amounts for Professional Services and a pro-rata portion of pre-paid Subscription Fees for the terminated Service(s). Either party may terminate this MSA and all SOs/SOWs if the other party becomes insolvent or ceases to conduct business without a successor.

10.4 **Effects of Expiration or Termination.** Upon the MSA's or an applicable SO's expiration or termination, Khoros will cease providing Services and Customer shall cease using the Services and delete, destroy, or return all copies of the Services documentation in its possession or control. The following survive expiration or termination: (a) any obligation of Customer to pay Fees or amounts incurred before expiration or termination; and (b) any provision of this MSA that expressly or by implication is intended to survive termination. If only a SO/SOW is expired or terminated, the other SOs/SOWs will remain in effect and this section will only apply to the expired or terminated SO/SOW.

10.5 **Transition Assistance.** After a SO concerning Khoros's Community product expires or terminates, Khoros will, if Khoros has not already done so on behalf of Customer, provide to Customer, at 1 time only and for no charge, Customer's Community content in standard industry format. For Khoros's other Services, Customer should access reporting, data, or exports (if any) during a SO's Term. The data will not be available for download after the end of a SO's Term. Customer agrees that downloadable content may only be available for extraction or downloading from certain Services for the most recent 18 months, that not all content is downloadable, and all content shall be retained and deleted in accordance with Khoros's data retention and deletion policies. Khoros may provide additional transition assistance at Khoros's standard rates for Professional Services.

10.6 **Data Deletion.** After a SO expires or terminates, Khoros will immediately suspend access to the Services. Within 30 days after such suspension, Khoros will permanently erase Customer Data and decommission Customer's account, with the following exceptions: (a) as otherwise required by applicable law; (b) data on backup systems is maintained for 90 days to maintain sound business continuity practices and then deleted; (c) log files are maintained for up to twelve months for security reasons and then deleted; or (d) as otherwise set forth in Khoros's current data retention and deletion policies.

11. MISCELLANEOUS

11.1 **Force Majeure.** No delay, failure, or default (other than a failure to pay Fees when due) will constitute a breach of this MSA and/or any SO/SOW to the extent caused by acts of war, terrorism, hurricanes, earthquakes, other acts of God or of nature, strikes or other labor disputes, riots or other acts of civil disorder, embargoes, government restrictions, changes in accessibility or terms of use of Social Media Networks, failure of third-party networks or services, failure of the public internet, or other causes beyond the performing party's reasonable control.

11.2 **Insurance**. Khoros will maintain commercially appropriate levels of insurance during the term of this MSA, including, but not limited to commercial and cyber insurance policies. Currently, Khoros maintains commercial and cyber insurance policies. Khoros shall provide a copy of its current insurance certificate to Customer upon written request.

11.3 **Technology Export.** Customer shall not: (a) allow itself or any third party to access or use the Services in violation of any US law or similar applicable regulation; or (b) allow or any third party to access or use the Services in, or export such software to, a country subject to a US embargo or sanction.

11.4 **Anti-Corruption.** Customer has not received or been offered any illegal bribe, kickback, payment, or unreasonable or unusual gift, or thing of value from any Khoros employee, agent, or representative in connection with this MSA, and any SO/SOW.

11.5 **Publicity.** With Customer's prior, written permission, Khoros may name Customer as a customer and use Customer's name, logo, and trademark in Khoros's promotional materials. Customer may request that Khoros stop doing so by sending an email to marketing@khoros.com.

11.6 **Independent Parties.** The parties are independent and neither is the representative or agent of the other; accordingly, neither may bind the other.

11.7 **Assignment & Successors.** Neither party may assign this MSA or SO/SOW, or any of its rights or obligations, without the other party's express written consent. However, either party may assign this MSA (and its attendant SOs/SOWs) pursuant to a merger, consolidation, or sale of substantially all its assets; provided however that Customer may not assign this MSA to a provider that competes with Khoros in the customer engagement software space.

11.8 **Notices.** Khoros will send notices under this MSA to Customer's email contact provided in a SO/SOW. Customer will send notices under this MSA to legal@khoros.com and to its Khoros customer success manager. Notices are considered received on the date that they are sent.

11.9 **Severability.** To the extent allowed by law, the parties waive any provision of law that would render any clause of this MSA invalid or otherwise unenforceable. If a provision of this MSA is held to be invalid or otherwise unenforceable, such provision will be interpreted to fulfill its intended purpose to the maximum extent allowed by applicable law, and the remaining provisions of this MSA will continue in full force and effect.

11.10 **No Waiver.** Neither party waives any of its rights under this MSA by lapse of time or by any statement or representation other than by an authorized representative in an explicit written waiver. No waiver of a breach of this MSA constitutes a waiver of any other breach of this MSA.

11.11 **Choice of Law & Jurisdiction.** This MSA and all related claims are governed by the laws of the State of Texas and applicable US federal law, without reference to: (a) any conflicts of law principle that would apply the substantive laws of another jurisdiction; (b) the 1980 United Nations Convention on Contracts for the International Sale of Goods; or (c) other international laws. The parties consent to the personal and exclusive jurisdiction of the federal and state courts of Austin, Travis County, Texas.

11.12 **Entire MSA.** This MSA and any related SO/SOW is the entire agreement of the parties and supersedes all prior or contemporaneous writings, written or oral negotiations, and oral discussions with respect to this MSA and Services. For the avoidance of doubt, Customer's purchase orders, vendor agreements and terms, online agreements, policies, or similar documents and terms, even if signed after this MSA and any SO/SOW, are not part of this MSA irrespective of what such orders, policies, and agreements provide about precedence.

11.13 **Amendments.** This MSA may only be amended by a written agreement signed by both parties that specifically references this MSA and is titled as an amendment.

11.14 **Order of Precedence.** The order of precedence is: the DPA, the SO/SOW, the MSA.

This MSA is agreed to By Customer. Customer Name: Customer Signature: Customer Signatory Name: Customer Signatory Title: Date of Signature:	**This MSA is agreed to by Khoros, LLC.** Khoros Signature: Khoros Signatory Name: Khoros Signatory Title: Date of Signature:

EXHIBIT A

KHOROS GLOBAL DATA PROTECTION AGREEMENT

This Data Protection Agreement (“DPA”) is an exhibit to and is incorporated by reference into the Master Services Agreement (“MSA”) between Khoros, LLC and its subsidiaries (collectively, “Khoros”) and the company/business entity that executed the MSA (“Customer”). This DPA only concerns personal data and does not amend or modify any terms in the MSA that are not specifically referenced in this DPA. In the event of a conflict between this DPA and the MSA, the terms of this DPA shall control. If a capitalized term is used in this DPA, but is not defined in the DPA, that term has the definition assigned to it under the Applicable Data Protection Law (defined below) or the MSA.

1. DEFINITION OF APPLICABLE DATA PROTECTION LAW. “Applicable Data Protection Law” or “ADPL” means any local, national or international laws, rules, and regulations related to privacy, security, data protection, and/or the processing of personal data, as amended, replaced or superseded from time to time including, but not limited to, the General Data Protection Regulation (“GDPR”), the California Consumer Privacy Act of 2018 (“CCPA”), the California Consumer Privacy Rights Act of 2020 (“CPRA”), the Colorado Privacy Act of 2020 (“CPA”), and the Virginia Consumer Data Protection Act of 2020 (“VDCPA”). The terms “Controller,” “Processor,” “Data Subject,” “Personal Data,” “Processing,” “Process,” and “Subprocessor” and all other similar or equivalent terms shall have the meanings given to them in the ADPL. In the event of a conflict between two or more ADPL with respect to the definition of such a term, the definition that affords the most protection to the Personal Data processed hereunder shall control.

2. PROTECTION OF PERSONAL DATA. With respect to the export of, access to, and Processing of Personal Data, both parties agree to comply with ADPL.

3. PROCESSING & THE ROLES OF THE PARTIES.

3.1 **Roles under ADPL**. Except as otherwise expressly stated in Section 3.2, the MSA, or elsewhere in this DPA:

(a) Customer is the Data Controller of Personal Data included in the Customer Data that is received by the Services;

(b) Customer hereby appoints Khoros as a Data Processor to Process the Personal Data included in the Customer Data; and

(c) Khoros shall Process Personal Data included in the Customer Data as a Data Processor as necessary to perform its obligations under the MSA, this DPA, and any SO and/or SOW (collectively, the “Agreement”) signed by the parties and strictly in accordance with the written instructions of Customer, except where otherwise required by any applicable law.

(d) The subject matter of the Data Processing is to provide, maintain, update, and improve the Services requested under the MSA. Khoros will Process Personal Data as necessary to provide the services under the MSA, and as further instructed by Customer. The duration of the Data Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Exhibit A.

Khoros shall immediately inform Customer, if, in Khoros’s opinion, any of Customer’s instructions violate ADPL. If Khoros is otherwise required to Process Personal Data included in the Customer Data pursuant to applicable law, Khoros will notify Customer without undue delay and the parties will cooperate to ensure such Personal Data is Processed to the minimum extent required by applicable law, unless such notification is prohibited by applicable law on important grounds of public interest.

3.2 **Roles under California Law.** The parties acknowledge and agree that Khoros is a Service Provider for the purposes of California law. Customer agrees to make Personal Data available to Khoros for the limited and specified purpose of performing its obligations under the Agreement signed by the parties and strictly in accordance with the written instructions of

Customer. Customer has the right to take reasonable and appropriate steps to help ensure that Khoros Processes Personal Data in a manner consistent with Khoros's obligations under ADPL. Upon notice, Customer also has the right to take reasonable and appropriate steps in accordance with the Agreement to stop and remediate any unauthorized processing of Personal Data. Khoros certifies that it understands the obligations and restrictions imposed on it by the CCPA and CPRA. Khoros will only collect, retain, use, disclose, and otherwise process Personal Information (as defined under the CCPA) to fulfil its obligations under the MSA, this DPA, on the Customer's behalf for business operational purposes, for Khoros's own operational purposes solely as permitted by the CCPA, or as otherwise permitted by the CCPA. Khoros will notify the Customer immediately if Khoros determines that it can no longer meet its obligations under ADPL or this DPA. Without limiting Khoros's obligations under this Section 3.2, Khoros shall not:

(a) share, sell, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, Personal Data to another person or entity for: (i) monetary or other valuable consideration; or (ii) cross-context behavioural advertising for the benefit of a business in which no money is exchanged; or

(b) combine Personal Data with Personal Data Khoros receives from or on behalf of another person or entity or collects from its own interactions with a Data Subject, unless such combination is required to perform a business purpose as defined in and as permitted by regulations adopted pursuant to Cal. Civ. Code 1798.185(10)(a).

If Khoros receives information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular Data Subject ("Deidentified Information") from Customer, or creates Deidentified Information at Customers instruction, Khoros will (a) take reasonable measures to ensure the Deidentified Information cannot be associated with a Data Subject or household, (b) publicly commit to maintain and use the Deidentified Information in deidentified form, and (c) not attempt to reidentify the Deidentified Information except for the sole purpose of determining whether Khoros' deidentification processes satisfy the requirements of ADPL.

4. TRANSFERS.

4.1 The parties agree that Customer's Personal Data Processed under this DPA may be transferred from the country of origin to the United States. Customer acknowledges that Khoros's primary Processing operations take place in the United States and that the transfer of Customer's Personal Data to the United States is necessary for the provision of the Services to Customer. In the event that Customer transfers Personal Data that is subject to: (i) the GDPR to Khoros outside of the EEA; (ii) the Swiss Federal Act on Data Protection to Khoros outside of Switzerland, (iii) the United Kingdom ("UK") General Data Protection Regulation (as implemented by the European Union (Withdrawal) Act 2018) ("UK GDPR") to Khoros outside of the UK, the parties agree that, as applicable to the Services, the associated Exhibit shall be deemed automatically incorporated into this DPA and binding upon the parties hereto, including their affiliates, unless an alternate data transfer arrangement authorized by ADPL is agreed by the parties. If the transfer is subject to Section 4.1(i) and/or Section 4.1(ii), Exhibit C shall apply. If the transfer is subject to Section 4.1(iii), Exhibit D shall apply. In the event of a conflict between the Agreement and an Exhibit, the Exhibit shall take precedence for any transfer of Personal Data made pursuant to this Section 4.

4.2 Insofar as the provision of the Services involve the transfer of Customer's Personal Data from any other jurisdiction where ADPL requires that additional steps, or safeguards, be imposed before the data can be transferred to a second jurisdiction, Khoros agrees, to the extent commercially practicable and at Customer's expense, to cooperate with Customer to take appropriate steps to comply with ADPL.

5. CONFIDENTIALITY. Khoros shall require that any Subprocessor or individual that has access to Personal Data be subject to a strict duty of confidentiality and prohibited from using the Personal Data for any purpose other than providing the Services (as defined in the MSA) or as otherwise expressly stated in the Agreement.

6. DATA SECURITY.

1. 6.1 **Security Practices.** Both parties shall maintain appropriate technical and organizational measures to protect the Personal Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of,

or access to the Personal Data (together referred to as a "Security Incident"). Khoros shall provide reasonable assistance to Customer for Customer to comply with its own obligations under the ADPL to maintain appropriate technical and organizational security measures.

6.2 **Security Incidents & Other Incidents.**

2.

(a) **Security Incident**. In the event of a confirmed Security Incident caused by Khoros, Khoros shall provide notice to Customer without undue delay and shall provide timely information and cooperation as required for Customer to fulfil its data breach reporting obligations under ADPL and other applicable law. Khoros shall further take all reasonable measures to remedy or mitigate the effects of the Security Incident and shall keep Customer informed of all such activities in connection with the Security Incident.

(b) **Other Incidents**. Security Incidents do not include any incident that results in no unauthorized access, destruction, loss, or alteration to Customer Data or to Khoros's Services, websites, or cloud servers involving pings and other broadcast attacks on firewalls or edge servers, phishing (even if successful), 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 not caused by any fault of Khoros. These incidents shall not be considered a breach of this DPA, the MSA, or SLA. Nonetheless, to the extent that a successful phishing attack leads to the compromise of Personal Data, Khoros will work with Customer to fulfil any ADPL reporting requirements.

6.3 **No Acknowledgement of Fault.** Khoros's obligation to report or respond to a Security Incident or other incident, if required by an ADPL, is not an acknowledgement by Khoros of any fault or liability of Khoros.

3.

6.4 **Audits.** Khoros shall conduct annual SSAE 18 SOC audit and/or maintain ISO 27001 certification during the term of Services. Khoros shall, upon request and on a confidential basis, provide Customer a valid ISO 27001 certificate or SSAE 18 SOC Type II audit report covering the Services. Customer agrees that the foregoing fulfils Khoros's audit obligations under ADPL, except for any additional audits required by an applicable data protection authority or regulatory body with authority over Khoros and/or Customer. To the extent legally required by ADPL, Khoros shall make available to Customer all information necessary to demonstrate Khoros's compliance with this DPA, as well as any ADPL.

7. RIGHTS OF DATA SUBJECTS. Khoros shall provide reasonable and timely assistance to Customer to respond to any request from a Data Subject to exercise a right relating to the Data Subject's Personal Data contained within the Customer Data. Khoros shall follow only Customer's instructions in this regard.

8. DATA PROTECTION IMPACT ASSESSMENTS ("DPIA"). If Khoros or Customer believe that the Processing by Khoros of the Personal Data contained within the Customer Data is likely to result in a high risk to the data protection rights and freedoms of Data Subjects, it shall promptly inform the other party. At Customer's sole cost and expense, Khoros shall provide Customer with all such reasonable and timely assistance necessary to conduct a DPIA, and if necessary, consult with its relevant data protection authority.

9. SUBPROCESSORS. Customer consents to Khoros engaging (and/or dismissing) Subprocessors to Process the Personal Data engaged as of the date of this DPA, and engaged or dismissed in the future, as deemed necessary by Khoros, provided that: (i) in relation to future Subprocessors, Khoros provides at least thirty (30) days' prior notice by posting at https://community.khoros.com/t5/Policies-and-Guidelines/What-companies-are-subprocessors-to-Khoros/ta-p/207777 and additionally provides thirty (30) days' prior notice via email and/or RSS feed notification to any of Customer's personnel who register (free of charge) at the aforementioned web page to receive such notifications; (ii) Customer may object to the addition of a new Subprocessor appointed by Khoros if Customer, in its reasonable discretion, believes that Khoros's use of such new Subprocessor would result in a violation of ADPL, in which case the parties agree to negotiate in good faith a mutually agreeable alternative. If no such alternative is agreed within two (2) months of the objection, Customer will have the right to terminate, without penalty, any services for which Personal Data would be processed by the new Subprocessor against which the objection was raised. Khoros shall require by written agreement each Subprocessor's compliance with the terms of this DPA and Khoros shall remain responsible for the Subprocessor's performance under the Agreement.

10. DELETION OR RETURN OF PERSONAL DATA. Upon the termination or expiration of the MSA, Khoros shall, and shall instruct all Subprocessors to, promptly (a) return to Customer or provide Customer the technical means to obtain all copies of Personal Data processed pursuant to Section 3.1(a) in Khoros's possession, or the possession of such Subprocessor, or (b) delete and procure the deletion of all other copies of Personal Data processed pursuant to Section 3.1(a) by Khoros or any Subprocessor. Khoros shall comply with all reasonable directions provided by Customer with respect to the return or deletion of such Personal Data. Notwithstanding the aforementioned, Khoros may retain Personal Data if required by ADPL, but only to the extent and for such period as required by such legal requirement. If required by law to retain Personal Data, Khoros shall continue to ensure the security and confidentiality of such Personal Data and only Process such Personal Data as necessary for the purpose specified in the ADPL requiring such storage.

11. LIABILITY. Khoros's liability for any non-compliance with this DPA shall be as follows:

(a) up to the maximum fine prescribed by ADPL with regard to fines and/or penalties imposed on Khoros or Customer by any data protection authority or governmental authority;

(b) regarding claims by Data Subjects, unlimited; and,

(c) for all other damages, as set forth in the MSA.

Exhibit A – Details of Data Processing Activities

This Exhibit A describes the Processing of Personal Data by Khoros acting as Data Processor on behalf of Customer.

SUBJECT MATTER	Khoros provides customer engagement software as a service to its customers.
CATEGORY OF DATA SUBJECTS	End users of Customer utilizing the technological solutions provided by the Khoros as described in the Agreement.
TYPE OF PERSONAL DATA	**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 DATA TRANSFERRED	N/A
FREQUENCY OF THE TRANSFER	☐ Data transferred on a one-off basis ☒ Data transferred on a continuous basis ☐ **Other:** ....
NATURE OF PROCESSING	Storage in encrypted format (strong AES encryption), secure transmission using HTTPS, secure access for support and troubleshooting purposes (VPN and secure Shell), usage tracking to provide reporting and metrics to Khoros customers (the data exporters).
PURPOSE OF THE PROCESSING	To provide data exporter, engineering and support services, and to transfer data to the subprocessors listed at the following URL: https://community.khoros.com/t5/Policies-and-Guidelines/What-companies-are-subprocessors-to-Khoros/ta-p/207777
PERIOD FOR WHICH THE PERSONAL DATA WILL BE RETAINED	Duration of the Agreement

Exhibit B – Supplementary Measures Khoros Uses Alongside SCCs To Protect EU Personal Information

Supplemental Measure	Description of What Khoros Does
Measures of pseudonymisation and encryption of Personal Data	We use a variety of masking and redaction technologies in our platforms **Where appropriate, sensitive data is masked from unauthorized users or redacted from our data set** **We also use encryption to protect the data sets and data transfers**
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of Processing systems and services	We use firewalls, access control lists, and Identity Access Management systems to limit access to Processing systems and services We use Web Application Firewalls and Intrusion Detection Systems to protect processing systems and services We have denial of service protections to assure availability We have multiple availability zones to improve resilience We make regular backups to assure the integrity of the data We conduct annual Disaster Recovery tests We employ application level monitoring to detect if systems operate outside of normal parameters
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	We backup data at least once per day We review, update, and test our disaster recovery plan annually
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the Processing	We conduct regular Static Security Scans of all source code We perform regular Dynamic Security Scans of all customer facing applications We train our employees on the OWASP Top 10 security vulnerabilities We deploy regular internal and external vulnerability scans We engage with third parties to conduct annual network and application penetration tests We complete an annual SOC 2 audit We complete an annual ISO27001 audit We complete an annual ISO27701 audit We complete an annual PCI audit for Secure Forms Service We complete an annual TRUSTe Privacy audit
Measures for user identification and authorization	We support the integration of any SAML 2.0 compliance Single Sign On system We support multi-factor authentication When local passwords are used, the passwords are salted and hashed before being stored
Measures for the protection of data during transmission	All data is encrypted in transit using TLS 1.2
Measures for the protection of data during storage	All data is encrypted at rest using AES 256
Measures for ensuring events logging	All application and infrastructure related security events are captured in our log aggregation system and are reviewed daily
Measures for ensuring system configuration, including default configuration	We use automation to assure that all systems are configured to standard We update our system images regularly to assure that they have the latest security patches
Measures for internal IT and IT security governance and management	We have a dedicated team that manages Security Risk, Compliance and Audits We conduct regular internal audits to confirm adherence to security policies We conduct regular security audits of all our vendors and subprocessors
Measures for ensuring data minimization	We strive to collect and maintain data necessary for our software and services, and for other reasons (e.g., security) that are aligned with industry custom and practice
Measures for ensuring limited data retention Measures for ensuring accountability	When Customer Data is no longer required, it is purged from our systems We delete backups after 90 days When the underlying infrastructure is decommissioned, it is done following the NIST 800-88 standard

Measures for allowing data portability and ensuring erasure	We provide a Data Access Request Form on our website (https://khoros.com/legal/data-protection-privacy)
Other protection measures	We maintain a law enforcement policy that describes how we will handle requests for personal information transferred from the EU

Exhibit C – EU Standard Contractual Clauses Module 2

The Parties agree that the following terms found in the EU Standard Contractual Clauses: Module 2 apply:

1. **Clause 7:** The Parties have chosen not to include Clause 7.

2. **Clause 9(a):** The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. 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 at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

3. **Clause 11:** The Parties incorporate the optional language allowing a data subject to lodge a complaint with an independent dispute resolution body at no cost to the data subject.

4. **Clause 13(a):** [Where the data exporter 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 the data exporter 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.

   [Where the data exporter 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.

5. **Clause 17:** 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.

6. **Clause 18(b):** The Parties agree that those shall be the courts of Ireland.

ANNEX I

A. LIST OF PARTIES

1. **Data exporter(s):** Customer, as identified in the Agreement
   Signature and date: Refer to Signatories of the DPA

   Role (controller/processor): data controller

2. **Data importer(s):** Khoros, LLC

   Signature and date: Refer to Signatories of the DPA

   Role (controller/processor): data processor

Activities relevant to the data transferred under these Clauses: For the purposes outlined in Sections 3.1 and 3.2 of the DPA.

B. DESCRIPTION OF TRANSFER

See Exhibit A.

C. COMPETENT SUPERVISORY AUTHORITY

Ireland.

ANNEX II

See Exhibit B.

ANNEX III – AMENDMENTS TO ENABLE THE TRANSFER OF DATA FROM SWITZERLAND TO A THIRD COUNTRY

Pursuant to the FDPIC's guidance titled "The transfer of personal data to a country with an inadequate level of data protection based on recognised standard contractual clauses and model contracts," dated 27 August 2021, the parties are adopting the GDPR standard for all data transfers under the FADP and under the GDPR. To the extent personal data is transferred outside of Switzerland to a country with an inadequate level of data protection, the following amendments to the Standard Contractual Clauses provided for in this Exhibit D shall apply:

1. Annex I.C: The competent supervisory authority shall be the FDPIC, insofar as the data transfer is governed by the FADP; and shall be the EU authority referenced in Annex I.C insofar as the data transfer is governed by the GDPR.
2. Applicable law for contractual claims under Clause 17 shall be Swiss law or the law of a country that allows and grants rights as a third party beneficiary for contractual claims regarding data transfers pursuant to the FADP; law of an EU member state for those according to the GDPR.
3. Place of jurisdiction for actions between the parties pursuant to Clause 18 b: Free choice for actions concerning data transfers pursuant to the FADP; court of an EU member state for actions concerning data transfers pursuant to the GDPR.
4. The term "member state" shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c).
5. Adjustments or additions regarding references to the GDPR: References to the GDPR should be understood as references to the FADP insofar as the data transfers are subject to the FADP.
6. The Standard Contractual Clauses shall also protect the data of legal entities until the entry into force of the revised FADP.

Exhibit D – UK International Data Transfer Agreement

1. Part 1: Tables

1. Table 1: Parties and signatures

Start date	Upon Execution of the DPA	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Customer, as identified in the Agreement	Full legal name: Khoros, LLC Trading name (if different): Main address (if a company registered address): 7300 Ranch Road 2222. Building 3, Ste. 150, Austin, TX 78730-3204 Official registration number (if any) (company number or similar identifier):
Key Contact	See Signatories of the DPA	See Signatories of the DPA
Importer Data Subject Contact	See Signatories of the DPA	See Signatories of the DPA
Signatures confirming each Party agrees to be bound by this IDTA	See Signatories of the DPA	See Signatories of the DPA

2. Table 2: Transfer Details

UK country's law that governs the IDTA:	☒ England and Wales ☐ Northern Ireland ☐ Scotland
Primary place for legal claims to be made by the Parties	☐ England and Wales ☐ Northern Ireland ☐ Scotland
The status of the Exporter	In relation to the Processing of the Transferred Data: ☒ Exporter is a Controller with respect to personal information referenced in Section 3.2 of the DPA. ☐ Exporter is a Processor or Sub-Processor
The status of the Importer	In relation to the Processing of the Transferred Data: ☐ Importer is a Controller ☒ Importer is the Exporter's Processor or Sub-Processor with respect to personal information referenced in Section 3.2 of the DPA. ☐ Importer is **not** the Exporter's Processor or Sub-Processor (and the Importer has been instructed by a Third Party Controller)
Whether UK GDPR applies to the Importer	UK GDPR applies to the Importer's Processing of the Transferred Data
Linked Agreement	The agreement(s) between the Parties which sets out the Khoros's instructions for Processing the Transferred Data are the Attached DPA and the Master Services Agreement.
Term	The Importer may Process the Transferred Data for the following time period: The period for which the Linked Agreement is in force.

Ending the IDTA before the end of the Term	The Parties cannot end the IDTA before the end of the Term unless there is a breach of the IDTA or the Parties agree in writing.
Ending the IDTA when the Approved IDTA changes	Which Parties may end the IDTA as set out in Section 29.2: ☒ Importer ☒ Exporter ☐ neither Party
Can the Importer make further transfers of the Transferred Data?	The Importer MAY transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data).
Specific restrictions when the Importer may transfer on the Transferred Data	The Importer MAY ONLY forward the Transferred Data in accordance with Section 16.1: ☐ if the Exporter tells it in writing that it may do so. ☐ to: ☐ to the authorised receivers (or the categories of authorised receivers) set out in: ☐ there are no specific restrictions. ☒ in accordance with Clause 9 of the EU SCCs
Review Dates	☐ No review is needed as this is a one-off transfer and the Importer does not retain any Transferred Data First review date: The Parties must review the Security Requirements at least once: ☐ each month(s) ☐ each quarter ☐ each 6 months ☐ each year ☐ each year(s) ☒ each time there is a change to the Transferred Data, Purposes, Importer Information, TRA or risk assessment

3. Table 3: Transferred Data

Transferred Data	The personal data to be sent to the Importer under this IDTA consists of the Personal Information outlined in Exhibit A. The categories of Transferred Data will update automatically if the information is updated in the Linked Agreement referred to.
Special Categories of Personal Data and criminal convictions and offences	The special categories personal data to be sent to the Importer under this IDTA consists of the Personal Information outlined in Exhibit A. The special categories of Transferred Data will update automatically if the information is updated in the Linked Agreement referred to.
Relevant Data Subjects	The Data Subjects of the Transferred Data are as outlined in Exhibit A. The categories of Data Subjects will update automatically if the information is updated in the Linked Agreement referred to.
Purpose	The Importer may Process the Transferred Data for the purposes set out in the Linked Agreement. The purposes will update automatically if the information is updated in the Linked Agreement referred to.

4. Table 4: Security Requirements

4. See Exhibit B.

2. Part 2: Extra Protection Clauses

See Exhibit B.

3. Part 3: Commercial Clauses

N/A

4. Part 4: Mandatory Clauses

Mandatory Clauses	Part 4: Mandatory Clauses of the Approved IDTA, being the template IDTA A.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 5.4 of those Mandatory Clauses.