



KHOROS EUROPE 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 (“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.

1. DEFINITION OF APPLICABLE DATA PROTECTION LAW. “Applicable Data Protection Law” or “ADPL” means the General Data Protection Regulation or “GDPR” and all other applicable laws and regulations governing the processing of personal data and data privacy and security that apply to Khoros. The terms “Controller,” “Processor,” “Data Subject,” “Personal Data,” “Processing,” “Process,” and “Subprocessor” have the meanings given to them in the ADPL.

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 Customer Data (Khoros as a Data Processor and Customer as a Data Controller). Except as otherwise expressly stated in the MSA:

- (i) Customer is the Controller of Personal Data included in the content that is received by the Applications;
- (ii) Customer hereby appoints Khoros as a Processor to Process the Personal Data included in the Customer Data; and
- (iii) Khoros shall Process Personal Data included in the Customer Data as a Processor as necessary to perform its obligations under the MSA and any service order (“SO”) and/or scope of work (“SOW”) signed by the parties and strictly in accordance with the written instructions of Customer, except where otherwise required by any applicable law.

Khoros shall immediately inform Customer, if, in Khoros’s opinion, any of Customer’s instructions violate ADPL. In the event that Khoros is otherwise required to Process Personal Data included in the Customer Data by 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 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 ADPL provisions applicable to Data Controllers.

3.3 Details of Khoros’s Processing. The subject matter of the 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. Processing will occur for the duration of the MSA, unless otherwise agreed in writing. The types of Personal Data and Data Subjects about which the Processing relates shall be as is contemplated or related to the Processing described in any SO and/or SOW that makes reference to, is incorporated under, or is subject to the MSA.

4. TRANSFERS.

4.1 European Economic Area Customer Data. Customer consents to the transfer of and/or access to Personal Data of European Economic Area (“EEA”) Data Subjects contained in the Customer Data by Khoros and/or Khoros’s Subprocessors to (or from) areas outside of the EEA provided that such transfer is carried out pursuant to the EC Standard Contractual Clauses -



Controller to Processor (the “Controller to Processor Clauses”), which are incorporated into and made part of this DPA. If requested by the Customer, Khoros agrees to sign such clauses and attach them as an exhibit to this DPA.

4.2 **Social Media Content.** To the extent Customer transfers any Personal Data contained in Social Media Content (as that term is defined in the MSA) to any country outside the EEA (except a country that is recognized under ADPL 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 DPA. Further, if ADPL requires or Customer requests, Khoros will sign physical copies of the Controller to Controller Clauses.

5. CONFIDENTIALITY.

5.1 Khoros as a Data Processor of Customer Data 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 MSA.

5.2 Customer as a Data Controller of Social Media Content shall require that any Subprocessor or individual that has access to Social Media Content complies with the applicable terms of use of the applicable social media platform from which the Social Media Content was originally obtained, and used, processed, stored, and disclosed only in accordance with applicable ADPL.

6. DATA SECURITY.

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 (“Security Incident”). Khoros shall provide reasonable assistance to Customer for Customer to comply with its own obligations under the APDL to maintain appropriate technical and organizational security measures.

6.2 Security Incidents & Other Incidents.

(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 to Customer Data (as defined in the MSA) or to Khoros’s Applications, 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.

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, 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’ 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.

7. RIGHTS OF DATA SUBJECTS. Khoros, as a Data Processor for Customer Data, shall provide reasonable and timely assistance to Customer to respond to any request from a Data Subject for the correction, updating, or deletion of the Data Subject’s Personal Data contained within the Customer Data. Khoros shall follow only Customer’s instructions in this regard. Each party in its role as a Data Controller shall comply with ADPL for Data Subject requests for retrieval, correction, or deletion of the Data Subject’s Personal Data contained within the Social Media Content under the control of a party.

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. If Khoros agrees that a DPIA is necessary, it 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 MSA, and engaged or dismissed in the future, as deemed necessary by Khoros, provided that: (i) in relation to future Subprocessors, Khoros provides at least 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 30 days prior notice via email notification to any of Customer’s personnel who register (free of charge) at the aforementioned web page to receive such notification; (ii) Customer may object to the addition of a new Subprocessor appointed by Khoros if Customer, in its reasonable discretion, believes that Khoros’ 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 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 this DPA and the MSA.

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

- a) up to the maximum fine prescribed by ADPL in regards to fines and/or penalties imposed on Khoros or Customer by any data protection authority or governmental authority;
- b) in regards to claims by data subjects, unlimited; and,
- c) for all other damages, as set forth in the MSA.

The individuals signing below hereby represent that they are each an authorized representative of their respective companies and have executed this DPA as of the last date of signature below. The Processing subject to this DPA shall continue until the MSA is terminated in accordance with the provisions set out in the MSA.

Customer

Khoros, LLC

Signature:

Signature:

Customer Name:

Signer’s Name:

Signer’s Name:

Title:

Title:

Date:

Date: