



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related to privacy, security, data protection, and/or the processing of personal data, as amended, replaced or superseded from time to time including, but not limited to, the General Data Protection Regulation (“GDPR”), the California Consumer Privacy Act of 2018 (“CCPA”), the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 Customer's 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.

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:	



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	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>
SENSITIVE DATA TRANSFERRED	N/A
FREQUENCY OF THE TRANSFER	<input type="checkbox"/> Data transferred on a one-off basis <input checked="" type="checkbox"/> Data transferred on a continuous basis <input type="checkbox"/> 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):** [insert customer name]
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

Identify the competent supervisory authority/ies in accordance with Clause 13

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	<p>Full legal name:</p> <p>Trading name (if different):</p> <p>Main address (if a company registered address):</p> <p>Official registration number (if any) (company number or similar identifier):</p>	<p>Full legal name: Khoros, LLC</p> <p>Trading name (if different):</p> <p>Main address (if a company registered address): 7300 Ranch Road 2222. Building 3, Ste. 150, Austin, TX 78730-3204</p> <p>Official registration number (if any) (company number or similar identifier):</p>
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:	<input checked="" type="checkbox"/> England and Wales <input type="checkbox"/> Northern Ireland <input type="checkbox"/> Scotland
Primary place for legal claims to be made by the Parties	<input type="checkbox"/> England and Wales <input type="checkbox"/> Northern Ireland <input type="checkbox"/> Scotland
The status of the Exporter	<p>In relation to the Processing of the Transferred Data:</p> <input checked="" type="checkbox"/> Exporter is a Controller with respect to personal information referenced in Section 3.2 of the DPA. <input type="checkbox"/> Exporter is a Processor or Sub-Processor
The status of the Importer	<p>In relation to the Processing of the Transferred Data:</p> <input type="checkbox"/> Importer is a Controller <input checked="" type="checkbox"/> Importer is the Exporter's Processor or Sub-Processor with respect to personal information referenced in Section 3.2 of the DPA. <input type="checkbox"/> 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: <input checked="" type="checkbox"/> Importer <input checked="" type="checkbox"/> Exporter <input type="checkbox"/> 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: <input type="checkbox"/> if the Exporter tells it in writing that it may do so. <input type="checkbox"/> to: <input type="checkbox"/> to the authorised receivers (or the categories of authorised receivers) set out in: <input type="checkbox"/> there are no specific restrictions. <input checked="" type="checkbox"/> in accordance with Clause 9 of the EU SCCs
Review Dates	<input type="checkbox"/> 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: <input type="checkbox"/> each [] month(s) <input type="checkbox"/> each quarter <input type="checkbox"/> each 6 months <input type="checkbox"/> each year <input type="checkbox"/> each [] year(s) <input checked="" type="checkbox"/> 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.
--------------------------	--