



Data Processing Agreement

(Article 28 GDPR)

Updated: May 7, 2026

This Data Processing Agreement ("DPA") forms part of the collaboration agreement ("Agreement") between **Keto Check, Inc. d/b/a Keto-Mojo** ("Controller") and the counterparty identified as the Partner in the Agreement ("Partner") regarding the processing of personal data in connection with services performed by Partner.

By executing the Agreement, Partner agrees to be bound by this DPA, which is incorporated into the Agreement by reference. In the event of any conflict between this DPA and the Agreement, this DPA shall govern with respect to the processing of Personal Data.

This DPA applies to the extent that Partner processes Personal Data connection with the Agreement, whether as a data processor acting on Controller's instructions (Module A) or as an independent data controller for its own clinical, research, or reporting purposes (Module B), that is subject to the **EU General Data Protection Regulation (EU) 2016/679 "GDPR"**, the **UK GDPR**, the **California Consumer Privacy Act (as amended by the CPRA) "CCPA"**, or any other applicable data protection law.

1. Definitions

The following definitions apply throughout this DPA:

Personal Data means any information relating to an identified or identifiable natural person, and includes "personal information" as defined under the CCPA and equivalent terms under other applicable privacy laws. For the avoidance of doubt, Personal Data processed under this DPA includes metabolic health data (including blood glucose and ketone measurements), device usage data, and any health-related information generated through use of the Keto-Mojo Solution.

Processing means any operation performed on Personal Data including collection, storage, organization, structuring, transmission, migration, or deletion.

Data Subject means the individual to whom the Personal Data relates, and includes "consumers" as defined under the CCPA.

Subprocessor means any third party engaged by Partner to process Personal Data on behalf of Controller

Personal Data Breach means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

Services means the services described in the Agreement.

Independent Controller Activities means processing of Personal Data by Partner for Partner's own clinical, diagnostic, treatment, research, or reporting purposes, including but not limited to: (a) incorporation of Personal Data into Partner's own electronic health records (EHR) system; (b) use of Personal Data for Partner's own clinical research or population health reporting; and (c) any other processing in which Partner independently determines the purpose and means of processing, as further described in Module B of Section 2.



Special Category Data means Personal Data revealing health information, as defined under GDPR Art. 9, including blood glucose measurements, ketone measurements, metabolic health data, and any other health-related data generated through use of the Keto-Mojo Solution. Such data constitutes “sensitive personal information” under CCPA § 1798.121.

2. Scope and Roles

This DPA governs two distinct processing relationships between Controller and Partner, each addressed in a separate Module. The applicable Module is determined by the nature of the processing activity as set forth below. Partner shall comply with the obligations of both Modules to the extent each applies to its activities.

Module A — Partner as Data Processor (Platform Access)

Module A applies where Partner accesses Personal Data solely through the Keto-Mojo Partner Interface, views data within Controller’s controlled platform environment, and does not independently store, export, or otherwise process Personal Data outside Controller’s systems.

Under Module A:

- Controller acts as the **data controller** (and “business” under the CCPA);
- Partner acts as the **data processor** (and “service provider” under the CCPA);
- Partner shall process Personal Data only on documented instructions from Controller, including as set forth in this DPA;
- Partner shall promptly inform Controller if, in its opinion, any instruction infringes applicable data protection law;
- Partner shall not: (a) sell Personal Data; (b) retain, use, or disclose Personal Data for any purpose other than performing the Services; (c) retain, use, or disclose Personal Data outside the direct business relationship between Partner and Controller; or (d) combine Personal Data with personal information received from other sources except as permitted by applicable law.

Module B — Partner as Independent Controller (EHR Export, Research, and Reporting)

Module B applies where Partner engages in Independent Controller Activities, including: (a) exporting or downloading Personal Data from the Keto-Mojo Partner Interface into Partner’s own systems or EHR; (b) using Personal Data for Partner’s own clinical research or population health reporting; or (c) any other processing in which Partner independently determines the purpose and means of processing.

Under Module B:

- Controller acts as the originating **data controller** for its own collection and platform-based processing of Personal Data;
- Partner acts as an **independent data controller** for its own Independent Controller Activities, and is independently responsible for compliance with all applicable data protection laws (including GDPR, UK GDPR, CCPA, and HIPAA) with respect to such activities;
- The disclosure of Personal Data by Controller to Partner for Independent Controller Activities constitutes a Controller-to-Controller data sharing arrangement governed by this Module B;



- Partner shall process Personal Data received under Module B only for the Permitted Purposes set forth in Section 2.1 below, and shall not use such data for any other purpose without Controller's prior written consent.

2.1 Permitted Purposes (Module B)

Partner may process Personal Data as an independent Controller solely for the following purposes ("Permitted Purposes"):

- Providing clinical care, treatment, and wellness services to the Partner's own patients or clients who are also Qualified End Users;
- Maintaining clinical records as required by applicable law, professional regulations, or institutional requirements;
- Conducting Partner's own de-identified or aggregated population health research and reporting, provided that Personal Data is de-identified in accordance with applicable law (including HIPAA Safe Harbor or Expert Determination standards, or GDPR pseudonymisation requirements) prior to use in research outputs;
- Internal quality improvement activities directly related to Partner's clinical services.

Partner shall not use Personal Data received under Module B for: (a) commercial purposes unrelated to the provision of clinical services to the relevant Data Subjects; (b) marketing or advertising; (c) sale or transfer to third parties except as permitted under Section 2.2; or (d) any purpose that would constitute a "sale" or "sharing" of personal information under the CCPA.

2.2 Onward Transfer Restrictions (Module B)

Partner shall not transfer, disclose, or otherwise make available Personal Data received under Module B to any third party except: (a) to Partner's own employees, contractors, and sub-processors who require access for the Permitted Purposes and are bound by obligations no less protective than those in this DPA; (b) as required by applicable law or court order, provided Partner gives Controller prompt prior written notice where legally permitted; or (c) with the prior written consent of Controller and, where required by applicable law, the relevant Data Subject.

2.3 Special Category Data (Both Modules)

The Parties acknowledge that Personal Data processed under this DPA may constitute Special Category Data. Each Party shall ensure that its processing of Special Category Data is supported by an appropriate legal basis under GDPR Art. 9(2) (or equivalent provisions under applicable law), which may include:

- Art. 9(2)(h): processing necessary for the purposes of preventive or occupational medicine, medical diagnosis, or the provision of health or social care treatment;
- Art. 9(2)(j): processing necessary for scientific or historical research purposes, subject to appropriate safeguards;
- Art. 9(2)(a): explicit consent of the Data Subject, where required.

Partner shall maintain records of its legal basis for processing Special Category Data and shall provide such records to Controller upon request.

3. Categories of Data and Data Subjects



The categories of Personal Data and Data Subjects processed under this DPA are set forth in Schedule 1, which may be updated by mutual written agreement of the parties as the scope of services evolves. Schedule 1 addresses both Module A and Module B processing activities separately.

4. Partner Obligations

Partner shall (under Module A):

- Process Personal Data only on documented instructions from Controller.
- Ensure that persons authorized to process Personal Data are bound by confidentiality obligations and are trained on applicable data protection requirements.
- Implement appropriate technical and organizational security measures to protect Personal Data, as further described in Section 6.
- Assist Controller, taking into account the nature of processing, in responding to Data Subject rights requests (including requests to know, delete, correct, or opt out under the CCPA) within a timeframe that enables Controller to meet its legal obligations, and in no event later than **5 business days** of receiving a request from Controller.
- Assist Controller in ensuring compliance with security, breach notification, data protection impact assessment, and prior consultation obligations under applicable law.
- Notify Controller **without undue delay, and in no event later than 48 hours**, after becoming aware of any Personal Data Breach affecting Personal Data processed under this DPA.
- Upon Controller's request, provide Controller with all information reasonably necessary to demonstrate Partner's compliance with applicable data protection law and this DPA.

Partner shall additionally (under Module B):

- Process Personal Data received under Module B only for the Permitted Purposes set forth in Section 2.1.
 - Implement and maintain technical and organizational security measures no less protective than those required under Section 6 of this DPA with respect to all Personal Data processed under Module B.
 - Notify Controller without undue delay, and in no event later than 48 hours, after becoming aware of any Personal Data Breach affecting Personal Data processed under Module B, regardless of whether Partner is acting as an independent Controller for that data.
 - Respond to Data Subject rights requests relating to Personal Data under Module B in Partner's possession independently, in compliance with applicable law. Where a Data Subject request requires action from Controller (e.g., deletion of data still held in Controller's systems), Partner shall notify Controller within 5 business days.
 - Maintain records of processing activities for Independent Controller Activities as required by GDPR Art. 30(1) (where applicable) and make such records available to Controller or any relevant supervisory authority upon request.
-

5. Subprocessors



Partner shall not engage any new Subprocessor without providing Controller with at least **14 days' prior written notice**, including the name, location, and nature of processing to be performed by the Subprocessor. Controller may reasonably object to the engagement of a new Subprocessor within such notice period, and the parties shall work in good faith to resolve any such objection.

Partner shall ensure that any Subprocessor is bound by data protection obligations no less protective than those in this DPA through a written agreement.

Partner remains fully liable to Controller for the performance and compliance of its Subprocessors under Module **A**.

A list of Partner's current Subprocessors that process Personal Data under this DPA (Module A) is set forth in Schedule 2, which Partner shall keep current and make available to Controller upon request.

6. Security Measures

Partner shall implement and maintain appropriate **technical and organizational measures** to protect Personal Data against:

- Unauthorized access
- Accidental or unlawful destruction
- Loss
- Alteration
- Unauthorized disclosure

At a minimum, such measures shall include: (a) encryption of Personal Data at rest and in transit; (b) access controls limiting Personal Data access to authorized personnel on a need-to-know basis; (c) regular testing and evaluation of the effectiveness of security measures; and (d) procedures for regularly restoring access to Personal Data in the event of a physical or technical incident.

Such measures shall be appropriate to the nature of the data and the risks involved in processing and shall be no less protective than industry-standard security practices. Given that Personal Data processed under this DPA may include Special Category Data, Partner's security measures shall be designed and implemented with particular regard to the sensitivity of health data and the risks of unauthorized access or disclosure.

7. Use of Test, Staging, or Development Environments

Partner shall ensure that any Personal Data used in testing, staging, or development environments is:

- Protected with **security controls equivalent to production systems**
- Limited to what is necessary for the applicable purpose, and where feasible, replaced with anonymized or pseudonymized data
- Not retained longer than necessary for that purpose, and deleted promptly upon completion of testing

8. Audit Rights

Controller, or a third-party auditor appointed by Controller, shall have the right, upon **reasonable prior written notice of at least 10 business days**, to audit partner's data processing activities and security practices to verify compliance with this DPA, no more than **once per calendar year** unless a Personal Data Breach has occurred or Controller has a reasonable, documented basis to suspect non-compliance.

Partner shall cooperate fully with such audits, provide access to relevant systems, documentation, and personnel, and promptly remediate any identified deficiencies.

The costs of any audit shall be borne by Controller unless the audit reveals material non-compliance by **Partner**, in which case Partner shall bear reasonable audit costs.

For the avoidance of doubt, Controller's audit rights under this Section extend to Partner's processing activities under both Module A and Module B, to the extent necessary to verify compliance with this DPA. Partner's obligation to cooperate with audits under Module B is limited to demonstrating compliance with the obligations set forth in this DPA; Controller does not have audit rights over Partner's broader business operations.

9. International Data Transfers

Partner shall not transfer Personal Data outside the United States or the European Economic Area without prior written authorization from Controller.

If a transfer outside these jurisdictions becomes necessary, the parties shall implement **appropriate safeguards** as required by applicable law, including:

- **Standard Contractual Clauses (SCCs)** as approved by the European Commission, for transfers subject to EU GDPR; and
- **The International Data Transfer Agreement (IDTA) or UK Addendum to the SCCs**, for transfers subject to UK GDPR.

Partner shall promptly execute any such transfer mechanisms upon Controller's request.

Where Partner processes Personal Data under Module B as an independent Controller and transfers such data outside the United States or EEA, Partner is independently responsible for implementing appropriate transfer safeguards under applicable law with respect to such transfers.

10. Data Retention and Deletion

Upon completion or termination of the Services, or upon Controller's earlier request, Partner shall, at Controller's choice and within **30 days**:

- Securely delete or destroy all Personal Data processed on behalf of Controller under Module A, or
- Return such Personal Data to Controller in a commonly used, machine-readable format,



and provide Controller with written certification of such deletion or return. Partner may retain Personal Data only to the extent required by applicable law, and shall notify Controller of any such retention obligation.

Notwithstanding the foregoing, the deletion and return obligations in this Section 10 apply solely to Personal Data processed under Module A. Personal Data that Partner has incorporated into Partner's own clinical records or EHR systems under Module B is subject to Partner's own data retention obligations under applicable law (including HIPAA, applicable state medical records laws, and professional regulations), and Controller's right to demand deletion does not extend to such data. Partner shall, however, upon termination of the Agreement, cease all new Independent Controller Activities and shall not request further data exports from Controller's systems.

11. Limitation of Liability

Each party's liability to the other under or in connection with this DPA shall be subject to the limitations and exclusions of liability set forth in the Agreement. Where the Agreement does not address liability for data protection matters, each party's aggregate liability under this DPA shall not exceed the greater of: (a) the total fees paid or payable by Controller to Partner in the **12 months preceding the event giving rise to the claim**; or (b) **\$100,000 USD**.

Notwithstanding the foregoing, neither party's liability shall be limited in the event of: (i) gross negligence or willful misconduct; (ii) a breach caused by Partner's failure to comply with its obligations under this DPA that results in a regulatory fine or penalty imposed on Controller; or (iii) any liability that cannot be limited by applicable law.

For the avoidance of doubt, each Party is independently liable for regulatory fines, penalties, and third-party claims arising from its own failure to comply with applicable data protection law in respect of its own processing activities. Controller's liability cap under this Section does not apply to Controller's obligations as originating Controller for Personal Data it collects directly from Data Subjects.

12. Compliance Information

Partner shall maintain complete and accurate records of all processing activities carried out on behalf of Controller (Module A) and, where required by applicable law, of all Independent Controller Activities (Module B), and shall make such records available to Controller or any relevant supervisory authority upon request.

13. Term

This DPA is incorporated into and effective upon execution of the Agreement. It remains in effect for the duration of the Agreement and survives termination to the extent necessary to ensure the return or deletion of Personal Data (as applicable under Sections 2 and 10) and any ongoing compliance obligations.



14. Governing Law

This DPA shall be governed by the governing law specified in the Agreement between the parties.

Schedule 1 – Details of Processing

Module A — Partner as Data Processor (Platform Access)

1. Subject Matter of Processing

Access to and review of End User metabolic health data through the Keto-Mojo Partner Interface, for the purpose of providing clinical and wellness services to Qualified End Users.

2. Nature and Purpose of Processing

Processing activities under Module A include:

- Viewing Qualified End Users' blood glucose and ketone measurements through the Partner Interface;
- Reviewing metabolic trends and health data to inform clinical consultations;
- Accessing device usage and measurement history within the Keto-Mojo platform;
- Any other access to Personal Data within the Keto-Mojo controlled platform environment as expressly authorized by Controller.

Processing is performed for the purpose of enabling Partner to provide clinical and wellness services to Qualified End Users who have consented to data sharing with Partner.

3. Categories of Personal Data (Module A)

May include, as applicable to the services performed:

- Name
- Email address
- Customer account identifiers
- Blood glucose measurements (date, time, value) — Special Category Data (GDPR Art. 9 / CCPA § 1798.121)
- Ketone measurements (date, time, value) — Special Category Data (GDPR Art. 9 / CCPA § 1798.121)
- Metabolic health and related health data and trends generated by or provided through the Keto-Mojo platform — Special Category Data
- Device usage data and activation history

4. Categories of Data Subjects (Module A)

May include, as applicable to the services performed:

- Qualified End Users: individuals who are both patients or clients of Partner and registered Keto-Mojo End Users who have provided informed consent for data sharing with Partner

5. Duration of Processing (Module A)



Partner will process Personal Data only for the duration necessary to perform the Services described in the Agreement, unless otherwise required by applicable law.

Module B — Partner as Independent Controller

The following details apply to Partner's Independent Controller Activities under Module B:

1. Subject Matter of Processing (Module B)

Partner's own clinical, diagnostic, treatment, research, and reporting activities using Personal Data received from Controller, including incorporation into Partner's EHR systems and use for population health research and reporting.

2. Nature and Purpose of Processing (Module B)

Processing activities under Module B may include:

- Export and import of Personal Data into Partner's electronic health records (EHR) system;
- Clinical documentation and care planning using metabolic health data;
- De-identified or aggregated population health research and reporting;
- Internal quality improvement analysis.

Processing is performed for Partner's own Permitted Purposes as defined in Section 2.1.

3. Categories of Personal Data (Module B)

As set forth in Schedule 1, Module A, Section 3, to the extent exported or otherwise transferred to Partner's systems. All such data retains its Special Category Data designation.

4. Categories of Data Subjects (Module B)

Qualified End Users for whom Partner provides clinical or wellness services and who have consented to the sharing of their Personal Data with Partner.

5. Duration of Processing (Module B)

Partner may retain Personal Data under Module B for the period required by applicable law, including HIPAA, applicable state medical records retention requirements, and professional regulations. Partner shall not retain Personal Data under Module B beyond the period required or permitted by such legal obligations.

Schedule 2 – Authorized Subprocessors

Partner shall maintain and provide to Controller upon request an up-to-date list of Subprocessors engaged to process Personal Data under this DPA (Module A), including for each: (a) the Subprocessor's name and contact information; (b) the country in which the Subprocessor processes Personal Data; and (c) a description of the processing performed.

Current Subprocessors as of the effective date of the Agreement are to be provided by Partner upon execution.