

TAOS

Privacy Policy

Effective date: June 1, 2026. Last updated: June 13, 2026.

Table of Contents

1. Introduction
2. Who We Are and How to Contact Us
3. When This Policy Applies
4. Key Definitions
5. Role of TAOS in Data Processing
6. Data We Collect
7. Sources of Data
8. Purposes for Which We Use Data
9. Legal Bases for Processing
10. Consent to Process Health Data and Share It with a Selected Professional
11. Integrations with Apple Health, Google Health Connect, Continuous Glucose Monitoring Systems, and Other Data Sources
12. Recipients of Data
13. Selected Professionals: Doctors, Clinics, Dietitians, Nutritionists, Fitness Trainers, and Other Professionals
14. Data Storage in Google Cloud and Firebase
15. International Data Transfers
16. Data Security
17. Data Retention
18. User Rights
19. Withdrawal of Consent and Account Deletion
20. Minor Users
21. Cookies, Analytics, and Marketing Communications
22. Payments, Subscriptions, and Paddle
23. Medical Disclaimer and Emergencies
24. Changes to This Policy
25. Contact Information

1. Introduction

1.1. This Privacy Policy (the “Policy”) explains what personal data and health data the TAOS platform collects and processes, the purposes for which the data is used, the persons to whom it may be disclosed, and the rights available to users.

1.2. TAOS is a technology platform for remote monitoring and transmission of a user’s health data to a doctor, clinic, dietitian, nutritionist, fitness trainer, nutrition professional, health and wellness professional, or another professional selected by the user. TAOS is not a healthcare provider, does not provide medical services, does not diagnose medical conditions, does not prescribe treatment, and does not replace consultation with a qualified doctor.

1.3. By using the website, mobile application, personal account, device integrations, or other TAOS services, you confirm that you have reviewed this Policy and understand how your data is processed.

1.4. If you do not agree with this Policy, do not use TAOS services and do not connect medical or other health-data sources.

1.5. This Policy forms an integral part of the [TAOS User Agreement](#). General terms for use of the Platform are governed by the TAOS User Agreement, while payment, subscription cancellation, and refunds are governed by the [TAOS Refund Policy](#).

2. Who We Are and How to Contact Us

2.1. The service is operated by TAOS Limited Liability Company (TAOS LLC), a company registered in the Republic of Armenia. Registered address: 18/2 Sevkaretsi Sako Street, Arabkir Administrative District, Yerevan 0012, Republic of Armenia. Registration number: 264.110.1483827 (referred to as “TAOS,” the “Company,” “we,” “us,” or “our”).

2.2. Questions concerning this Policy, the processing of personal data, account deletion, withdrawal of consent, or the exercise of user rights may be submitted through the following contact channels:

- Support email: support@taos.health
- Website: <https://www.taos.health>
- Related documents: [TAOS User Agreement](#); [TAOS Refund Policy](#).

2.3. If the appointment of a representative or data-protection officer is required in the user’s jurisdiction, the relevant information will be published on the TAOS website or provided in response to a request submitted to Support.

3. When This Policy Applies

3.1. This Policy applies to use of:

- the TAOS mobile application;
- the TAOS website;
- the patient’s personal account;
- the dashboard of a doctor, clinic, or other Selected Professional;
- features connecting devices, continuous glucose monitoring systems (CGM), glucose meters, Apple Health, Google Health Connect, and other data sources;
- TAOS Support and communications with TAOS;
- payment and subscription-management features provided through the website, application, or a Payment Provider.

3.2. This Policy does not govern the independent activities of doctors, clinics, dietitians, nutritionists, fitness trainers, nutrition professionals, health and wellness professionals, insurance companies, device manufacturers, Payment Providers, or other third parties where they process data under their own privacy policies and legal obligations.

4. Key Definitions

4.1. “Personal Data” means any information relating directly or indirectly to an identified or identifiable person.

4.2. “Health Data” or “Medical Data” means information concerning physical condition, health indicators, laboratory results, continuous glucose monitoring (CGM) data, glucose meter data, health devices and applications, symptoms, medications, and other information related to the user’s health.

4.3. “User” means a person who creates an account, connects data sources, uses the TAOS service, or provides data for transmission to a Selected Professional.

4.4. “Selected Professional” means a doctor, clinic, healthcare organization, dietitian, nutritionist, fitness trainer, nutrition professional, health and wellness professional, or another professional or organization independently selected or connected by the user through TAOS to view the user’s data. If the professional is not a licensed healthcare professional, their services do not constitute medical consultation, diagnosis, or treatment.

4.5. “Doctor” or “Healthcare Professional” means an independent licensed healthcare practitioner, clinic, or healthcare organization selected by the user to receive the user’s data through TAOS.

4.6. “Processing” means any operation performed on data, including collection, recording, storage, organization, transmission, deletion, de-identification, and protection.

4.7. “Integrations” means technical connections to Apple Health, Google Health Connect, continuous glucose monitoring systems (CGM), glucose meters, wearable and medical devices, application programming interfaces (API), or other data sources voluntarily connected by the user.

5. Role of TAOS in Data Processing

5.1. When processing data related to user accounts, operation of the application, subscriptions, technical support, and general service administration, TAOS usually acts as the data controller.

5.2. With respect to data transmitted by a user to a Selected Professional, TAOS provides technical infrastructure for transmission, display, and organization of the data. The professional may act as an independent data controller in the course of professional activities and under applicable law.

5.3. TAOS does not make medical, dietary, nutrition, fitness, wellness, or other professional decisions on behalf of a Selected Professional, does not control treatment, and does not replace a clinic’s medical records. TAOS is not responsible for the independent acts or omissions of a Selected Professional unless mandatory law provides otherwise.

5.4. If TAOS acts as a data processor on behalf of a clinic, doctor, dietitian, nutritionist, fitness trainer, insurance company, or another partner, the processing terms are governed by a separate agreement between TAOS and that partner.

6. Data We Collect

6.1. Account Data

- first and last name;
- email address;
- telephone number;
- country, city, or region where necessary for operation of the service;
- interface language;
- account identifier;
- password or other credentials in protected form;
- information about the selected subscription plan.

6.2. Health and Monitoring Data

TAOS may process the following data where you enter it manually, upload it, or connect the relevant data source:

- glucose levels and glucose trends;
- continuous glucose monitoring (CGM) data, including time series, trends, and events;
- glucose meter data;
- weight, body mass index, and other anthropometric indicators;
- physical activity, steps, workouts, and energy-expenditure data;

- sleep data;
- heart rate and other indicators where the user has connected the relevant source;
- information about nutrition, symptoms, wellbeing, medications, or other events where the user uses the relevant feature;
- documents uploaded by the user where this feature is available, including laboratory results, medical records, images, or other medical files;
- comments, notes, and data entered directly by the user into the service.

6.3. Data from Devices and Integrations

If a user connects Apple Health, Google Health Connect, a continuous glucose monitoring system (CGM), a glucose meter, a wearable device, or another data source, TAOS receives only the categories of data that the user has authorized in the relevant interface.

6.4. Selected Professional Data

- name and contact details of the Selected Professional;
- identifier of the Selected Professional in TAOS;
- list of users or patients connected to the Selected Professional through TAOS;
- comments by the Selected Professional, monitoring statuses, or administrative notes where the relevant feature is enabled;
- information about the user's subscription to monitoring by a particular Selected Professional where this model is used.

6.5. Payment and Subscription Data

TAOS may process information about the subscription plan and status, purchase and renewal dates, cancellation and refund statuses, and transaction identifiers. Full payment-card data is generally processed by the Payment Provider and is not stored in full in TAOS systems.

6.6. Technical Data

- IP address;
- device type;
- operating system;
- application version;
- language and regional settings;
- device or session identifiers;
- error logs;
- account-login data;
- information about actions within the application that is required for security, support, and service improvement.

6.7. Communications with Support

If a user contacts TAOS Support, we may retain the content of the request, contact details, attachments, and communication history to process the request and protect the rights of the parties.

6.8. De-identified and Aggregated Data

TAOS may create de-identified or aggregated data that does not identify a specific user. Such data may be used for statistics, product improvement, assessment of service quality, and development of features. TAOS does not use identifiable health data for advertising without the user's separate explicit consent.

7. Sources of Data

7.1. We obtain data from the following sources:

- directly from the user during registration, profile setup, manual data entry, or communications with Support;
- from data sources connected by the user, including Apple Health, Google Health Connect, continuous glucose monitoring systems (CGM), glucose meters, wearable devices, and other integrations;
- from the professional selected by the user where the professional uses the TAOS dashboard;
- from Payment Providers, app stores, or partners involved in processing subscriptions;
- from technical logs of the application and website.

7.2. The user controls the connection of most medical-data and physical-activity data sources. Permissions may be withdrawn through device settings, application settings, Apple Health, Google Health Connect, or the TAOS account where the relevant feature is available.

8. Purposes for Which We Use Data

8.1. TAOS uses data only for purposes related to operation of the service, security, support, legal obligations, and product improvement. The principal processing purposes are:

- creating and maintaining the user's account;
- connecting data sources and synchronizing indicators;
- organizing and displaying user data in the application;
- transmitting data to the professional selected by the user;
- providing the Selected Professional with a monitoring dashboard and access to data of connected users or patients;
- processing subscriptions, cancellations, payment statuses, and refunds;
- providing technical support to the user and the Selected Professional;
- maintaining account security and preventing abuse and unauthorized access;
- correcting errors, testing, and improving application stability;
- performing de-identified product analytics and compiling usage statistics;
- complying with applicable law, Payment Provider requirements, app-store rules, and lawful requests from public authorities.

8.2. TAOS does not use health data obtained from Apple Health, Google Health Connect, continuous glucose monitoring systems (CGM), glucose meters, or other medical sources for targeted advertising, sale to advertisers, or creation of advertising profiles.

9. Legal Bases for Processing

9.1. Depending on the user's country and the type of data, TAOS may process data on the following legal bases:

- User consent: for processing health data, connecting data sources, transmitting data to a Selected Professional, and certain marketing communications.
- Performance of a contract: to create an account, provide access to the Platform, manage a subscription, and provide technical support.
- Legitimate interests: to maintain security, prevent fraud, improve the product, perform internal analytics, and protect TAOS rights, where those interests do not override the user's rights.
- Legal obligation: to comply with applicable law, tax requirements, Payment Provider requirements, app-store rules, and lawful requests from public authorities.
- Protection of vital interests: in exceptional cases where processing is necessary to protect the life or safety of the user or another person and is permitted by law.

9.2. Health data is a sensitive category of data. TAOS processes such data only where an appropriate legal basis exists, usually the user's explicit consent or another lawful basis permitted by applicable law.

10. Consent to Process Health Data and Share It with a Selected Professional

10.1. By connecting data sources, entering health indicators, or selecting a doctor, clinic, dietitian, nutritionist, fitness trainer, or another professional for monitoring, the user consents to TAOS processing the relevant data and transmitting it to the Selected Professional within the functionality of the service.

10.2. Consent must be freely given, specific, informed, and expressed by an affirmative action, such as clicking a button, selecting a checkbox, confirming within the application, or granting permission through Apple Health, Google Health Connect, or another data-source interface.

10.3. The user understands that the Selected Professional will be able to view data transmitted through TAOS to the extent necessary for monitoring and interaction with the user in the course of the professional's activities.

10.4. The user may withdraw consent to transmission of data to a Selected Professional by disconnecting the professional in the application or submitting a request to Support. Withdrawal does not affect the lawfulness of processing carried out before withdrawal.

10.5. If a user withdraws consent or disconnects a data source, certain TAOS features may become unavailable or operate on a limited basis.

11. Integrations with Apple Health, Google Health Connect, Continuous Glucose Monitoring Systems, and Other Data Sources

11.1. General Integration Rules

TAOS obtains data from external sources only after receiving the user's permission. The user may manage permissions through device settings, Apple Health, Google Health Connect, device-manufacturer applications, or TAOS settings where the relevant feature is available.

11.2. Apple Health

If a user connects Apple Health, TAOS requests access only to the types of data required for the relevant features. TAOS does not use data obtained through Apple Health for advertising, sale to third parties, or purposes unrelated to the stated service functionality.

11.3. Google Health Connect

If a user connects Google Health Connect, TAOS requests only the permissions required to provide the stated features. Health Connect data is used only for application functionality, transmission to the Selected Professional, and related service purposes. The user may withdraw permissions through Health Connect settings.

11.4. Continuous Glucose Monitoring Systems, Glucose Meters, and Other Devices

If a user connects a continuous glucose monitoring system (CGM), glucose meter, or another device, processing may also be governed by the terms and policies of the device manufacturer or relevant platform. TAOS does not control the independent activities of those third parties.

11.5. Data Minimization

TAOS requests only the minimum amount of data necessary for the relevant features and does not request excessive permissions.

12. Recipients of Data

12.1. TAOS may disclose data to the following categories of recipients:

- Selected Professional: data is transmitted only for the monitoring selected by the user or connection to a doctor, clinic, dietitian, nutritionist, fitness trainer, nutrition professional, health and wellness professional, or another professional.
- Google Cloud and Firebase: infrastructure for data storage and processing, user authentication, backups, technical logs, and operation of the application.
- Payment Providers: for example, Paddle, App Store, Google Play, or other providers involved in processing payments, subscriptions, refunds, and tax obligations.
- Technical service providers: hosting and infrastructure support, error analysis, support services, email and mobile notifications, stability monitoring, and security.
- Device manufacturers and integration platforms: where the user connects the relevant integration and disclosure is necessary for it to operate.
- Public authorities or courts: only where required by applicable law, a lawful request, or protection of the rights of TAOS, users, or third parties.
- Corporate transaction partners: in connection with a reorganization, asset sale, investment, merger, or other corporate transaction, subject to applicable law and data-protection requirements.

12.2. TAOS does not sell users' personal data or health data to advertisers, data brokers, or other third parties.

12.3. Transmission of data to a professional selected by the user is not a sale of data because it occurs at the user's direction and for the monitoring feature selected by the user.

13. Selected Professionals: Doctors, Clinics, Dietitians, Nutritionists, Fitness Trainers, and Other Professionals

13.1. Doctors, clinics, dietitians, nutritionists, fitness trainers, nutrition professionals, health and wellness professionals, and other professionals using TAOS are independent professionals or organizations and are not part of TAOS. They are not employees, agents, or representatives of TAOS unless a written agreement expressly provides otherwise.

13.2. Licensed doctors, clinics, and healthcare organizations are independently responsible for medical decisions, consultations, interpretation of data, maintenance of medical records, professional standards, and compliance with healthcare law. Dietitians, nutritionists, fitness trainers, and other non-medical professionals are independently responsible for their recommendations and services within their qualifications and must not present those services as medical diagnosis or treatment unless appropriately licensed.

13.3. After data is transmitted to a Selected Professional, the recipient may process it under their own legal obligations, professional rules, and privacy policies. The user may ask the Selected Professional how the received data is processed.

13.4. TAOS may restrict a Selected Professional's access to user data if the user disconnects the professional, cancels a subscription, or withdraws consent, except where continued retention or processing is required by law.

14. Data Storage in Google Cloud and Firebase

14.1. TAOS uses Google Cloud Platform and, where necessary, Firebase infrastructure to store and process data and operate the service. These services act as technical-infrastructure providers and generally process data on behalf of TAOS under applicable data-processing terms.

14.2. Use of Google Cloud and Firebase does not mean that Google independently determines the purposes for processing the user's medical data. Processing purposes are determined by TAOS and/or the relevant Selected Professional according to each party's role.

14.3. TAOS may use Google Cloud and Firebase for:

- storage of account data and health data;
- user authentication;
- databases and data synchronization;
- backups;
- technical-event logging;
- application-stability and error analytics;
- security and access control.

14.4. TAOS is designed with privacy and security principles in mind. Compliance with the EU General Data Protection Regulation (GDPR), the U.S. Health Insurance Portability and Accountability Act (HIPAA), or other legal regimes depends not only on the cloud provider, but also on application architecture, contracts, access settings, internal procedures, and legal assessment.

14.5. If TAOS processes protected health information in the United States in circumstances where HIPAA applies, the Company will implement the necessary contractual and technical measures, including entering into a HIPAA Business Associate Agreement where required by applicable law and the parties' roles. Unless separately confirmed in writing, TAOS does not represent that the service is fully HIPAA compliant in every use scenario.

15. International Data Transfers

15.1. User data may be stored and processed outside the user's country of residence depending on the location of Google Cloud and Firebase infrastructure, Payment Providers, Support, the Selected Professional, and other service providers.

15.2. Where applicable law requires specific mechanisms for international data transfers, TAOS uses appropriate contractual, technical, and organizational safeguards, such as standard contractual clauses, data-processing agreements, access restrictions, and other protective measures.

15.3. By using the service and connecting a Selected Professional located in another country, the user understands that data may be transferred to that country for monitoring and interaction with the Selected Professional.

16. Data Security

16.1. TAOS applies reasonable technical and organizational safeguards taking into account the nature of the data, risks, and available technologies. Such measures may include:

- encryption of data in transit;
- encryption of data at rest where applicable and supported by the services used;
- role-based access restrictions;
- user authentication;
- logging of technical actions and security events;
- backups;
- monitoring of errors and incidents;
- limiting Selected Professionals to data of their connected users or patients;
- internal access rules for employees and contractors;
- security-incident response procedures.

16.2. Despite these measures, no transmission or storage method is completely secure. The user is also responsible for the security of their device, password, email address, and account access.

16.3. If a security incident occurs, TAOS will take reasonable steps to investigate and mitigate it and will notify users and regulators where notification is required by applicable law.

17. Data Retention

17.1. TAOS retains data for as long as necessary for the purposes described in this Policy. Longer retention is permitted where required by law, contract, tax rules, Payment Provider rules, or protection of the parties' rights.

17.2. The principal indicative retention periods are set out below:

Data category	Indicative retention period	Comment
Account data	While the account remains active and for a reasonable period after deletion	For account recovery, security, disputes, and legal obligations.
Health data	While the account remains active or until the user requests deletion	May be retained longer where required by law or an agreement with a doctor or clinic.
Payment records	For the period required by tax and payment law	TAOS generally does not store full payment-card data.
Technical logs	For a limited period required for security and diagnostics	The specific period depends on system settings.
De-identified data	May be retained for a longer period	Must not permit identification of the user.

17.3. If a user deletes an account or withdraws consent, TAOS deletes or de-identifies the data within a reasonable period, except where continued retention is required by law, performance of a contract, protection of rights, fraud prevention, or technical backup limitations.

18. User Rights

18.1. Depending on applicable law, the user may have the following rights:

- the right to obtain information about the data being processed;
- the right to request a copy of the user's data;
- the right to correct inaccurate data;
- the right to delete data or the account;
- the right to restrict processing;
- the right to withdraw consent;
- the right to object to processing;
- the right to data portability;
- the right to lodge a complaint with a competent data-protection authority;
- the right not to be subject to a solely automated decision producing legal or similarly significant effects, where such a right is provided by law.

18.2. To exercise rights, the user may send a request to Support at support@taos.health.

18.3. TAOS may request verification of the user's identity before acting on a request in order to protect data from unauthorized access.

18.4. If a request concerns data already transmitted to a Selected Professional, TAOS may also direct the user to that professional because the professional may independently be responsible for part of the processing.

19. Withdrawal of Consent and Account Deletion

19.1. A user may withdraw consent to processing health data, disconnect individual data sources or a Selected Professional, and request deletion of the account.

19.2. Withdrawal of consent may make certain TAOS features unavailable, including monitoring, transmission of data to a Selected Professional, display of trends, and device synchronization.

19.3. To delete an account, the user must send a request to Support at support@taos.health.

19.4. After account deletion, some data may remain for a limited period in backups, payment records, security logs, or legally required archives. Access to such data is restricted, and the data is deleted or de-identified as the relevant retention periods expire.

20. Minor Users

20.1. TAOS is intended for users who have reached the age at which they may independently consent to personal-data processing in their country. Where applicable law requires consent from a parent or legal guardian, TAOS may be used only with that consent.

20.2. TAOS is not intended for independent use by children under 13. Higher age thresholds, including 16, may apply to users in the European Economic Area, the United Kingdom, or other regions where required by local law.

20.3. If TAOS learns that a minor's data was provided without required parental or guardian consent, TAOS will take reasonable steps to delete the data or restrict its processing.

21. Cookies, Analytics, and Marketing Communications

21.1. The TAOS website and application may use small browser-stored files (cookies), software development kits (SDKs), pixels, local storage, and similar technologies for account login, security, remembering settings, technical diagnostics, and product analytics.

21.2. TAOS may use de-identified or aggregated analytics to understand how users interact with the service, identify unstable features, and improve the product.

21.3. TAOS does not use user health data obtained from medical sources, Apple Health, Google Health Connect, continuous glucose monitoring systems (CGM), or glucose meters for targeted advertising or sale to advertisers.

21.4. Marketing emails or mobile notifications are sent only where there is an appropriate legal basis and an option to opt out. Service communications relating to security, subscriptions, changes to terms, or account operation may be sent regardless of marketing preferences.

22. Payments, Subscriptions, and Paddle

22.1. If a user purchases a subscription through the TAOS website, payment may be processed by Paddle or another Payment Provider. If a subscription is purchased through App Store or Google Play, payments and refunds may be governed by the relevant app-store rules.

22.2. TAOS may receive limited transaction information from the Payment Provider, including payment status, amount, currency, date, subscription status, cancellation or refund status, tax information, and transaction identifier. Full payment-card details are processed by the Payment Provider and are generally not provided to TAOS in full.

22.3. Subscription cancellation and refund rules are set out in the [TAOS User Agreement](#) and the [TAOS Refund Policy](#). TAOS may voluntarily accept a request for refund of the initial subscription payment within

three calendar days unless a different period is required by applicable law, Payment Provider rules, or app-store rules.

22.4. This Policy does not limit mandatory consumer rights under applicable law.

23. Medical Disclaimer and Emergencies

23.1. TAOS is a technology platform for collecting, organizing, and transmitting data to the user and a Selected Professional. TAOS does not provide medical consultations, diagnose medical conditions, prescribe treatment or medicines, issue prescriptions, or provide emergency medical care.

23.2. Data, charts, notifications, and other information in TAOS must not be used as the sole basis for medical decisions. The user must consult a qualified doctor regarding diagnosis, treatment, changes to medication regimens, or other medical management. Recommendations from a dietitian, nutritionist, fitness trainer, or another non-medical professional do not replace medical consultation where a disease, symptoms, or medical risks exist.

23.3. If a user believes that a medical emergency has arisen, the user must immediately contact local emergency services or the nearest healthcare facility. TAOS is not intended for emergencies.

24. Changes to This Policy

24.1. TAOS may update this Policy periodically to reflect changes in the product, applicable law, payment model, integrations, or data-processing practices.

24.2. If changes are material, TAOS will take reasonable steps to notify users, for example by email, mobile notification, in-application message, or publication on the website.

24.3. Continued use of the service after an updated Policy takes effect constitutes acceptance of the updated terms unless applicable law provides otherwise.

25. Contact Information

For all questions concerning this Policy, data processing, an account, or use of the service, the user may contact TAOS through Support or the website:

Matter	Contact
Support, privacy, user rights, and account deletion	support@taos.health
Website	https://www.taos.health