Open Wearables Connect

Privacy Policy

Effective date: 11.11.2026.

1. Who we are and what this policy covers

Open Wearables Connect (the "**App**") sends health and fitness data from your phone to the healthcare provider, clinic, coach or other organization that invited you (the "**Organization**"). The App is published by Momentum Sp. z o.o. with its registered address in Poland, Wrocław (53-659), at ul. Gen. Władysława Sikorskiego 26, entered in the Register of Entrepreneurs of the National Court Register maintained by the District Court for Wrocław Fabryczna in Wrocław, 7th Commercial Division of the National Court Register, under KRS number: 0000602983 ("**Momentum**", "**we**", "**us**").

Two different parties are responsible for your data:

- **The Organization** decides which health data it receives and what it does with it. It runs its own server, and your health data goes there directly. For that data, the Organization is the controller, and its own privacy notice applies.
- **Momentum** only checks that the Organization holds a valid subscription. For the small set of technical data used for that check (described in section 4), we are the controller.

This policy explains both. It covers only the App. It does not cover the Organization's own systems, Apple Health, Google Health Connect, or the wearable devices you use.

If you live in the United States, our Consumer Health Data Privacy Policy is in section 10.

2. How the App works

The App moves your data from your phone to the Organization's server; it does not route your health data through Momentum.

1. The Organization invites you by email, with a link or a QR code.
2. You install the App and open the link or scan the code. The App connects to the Organization's server named in the invitation.
3. You choose which data types to share in Apple Health (iOS) or Health Connect (Android).
4. The App reads the data you allowed and sends it, encrypted, directly to the Organization's server. It does this periodically in the background.
5. When you connect, and periodically afterwards, the App asks our license server whether the Organization's subscription is valid. This check never includes health data.

You can stop sharing at any time (see sections 7 and 8).

3. Your health data

Momentum never receives, stores or has access to your health data; it goes only from your phone to the Organization.

What the App reads. The App reads only the data types you approve in Apple Health or Health Connect. It asks for: activity (steps, distance, floors climbed, walking and running metrics); workouts, including their duration, energy, heart rate, power and cadence, and on iOS the GPS route of each workout; energy burned; heart (heart rate, resting heart rate, heart rate variability, recovery, VO2 max); blood oxygen and respiratory rate; body measurements (weight, height, BMI, body fat, lean mass, waist circumference, body temperature); blood pressure, blood glucose and insulin delivery; nutrition and hydration; sleep and mindfulness sessions; and reproductive health (menstrual flow, cervical mucus, ovulation tests, sexual activity). Which of these exist on your phone depends on your devices and on the platform: some types are available only on iOS. You can approve or refuse each type separately, and the App works with whatever you approve. The App does not write any data into Apple Health or Health Connect.

Where it goes. The App sends the data over an encrypted connection (TLS) to the server address in your invitation. That server is run by the Organization, which decides where it is located and how long it keeps your data. Until a send succeeds, data waiting to be sent is kept only on your phone, in the App's private storage.

Who is responsible. The Organization is the controller of your health data. Questions about how it is used, kept or shared, and requests to access or delete it, go to the Organization. Its privacy notice should be available from the Organization or in the invitation it sent you. We cannot see, change or delete data held by the Organization.

4. Data Momentum processes

We process only the technical data needed to check the Organization's license and keep the service secure.

Data	Why we use it	How long we keep it
Pseudonymous user ID (a random code assigned when you connect; it contains no name, email or health data)	To link license checks to one connected user and count active users under the Organization's subscription	While you stay connected, then 30 days after the last license check

Data	Why we use it	How long we keep it
Installation ID (a random code created when the App is installed)	To tell installations apart and to detect misuse of a license	While you stay connected, then 30 days after the last license check
Platform (iOS or Android) and App version	To check compatibility and support older App versions	Same as the installation ID
IP address and time of each check	To deliver the response, protect our servers and investigate abuse	30 days in server logs
Organization identifier (a random code that identifies the Organization's server in our license system, together with its subscription plan)	To find the Organization's subscription and check that it is valid	While you stay connected, then 30 days after the last license check

Legal basis. We process this data because we have a legitimate interest in verifying that the App is used under a valid subscription, preventing misuse and keeping our systems secure. Where a law requires us to state a legal basis, this is Article 6(1)(f) of the EU and UK GDPR or the equivalent legitimate-interest provision of other applicable law. Where a law requires consent instead, we rely on the consent you give when you connect the App. You can object to this processing, or ask how we weighed our interests against yours (section 9).

Identification. We do not know your name, email address or the Organization's internal records about you. We do not try to identify you from this data. We do not use the IP address to work out your location.

5. What we do not do

- We do not receive, store or analyse your health data on our servers.
- We do not use any data from the App, including data from Apple HealthKit or Health Connect, for advertising, marketing or profiling.
- We do not sell or rent your data, and we do not share it for cross-context behavioral advertising.
- We do not track you across other companies' apps or websites.
- The App does not store health data in iCloud or any other cloud backup.
- The App contains no third-party analytics, advertising or crash-reporting tools.

Data obtained through Health Connect is used only to provide the App's syncing feature to you, in line with the Health Connect Permissions policy and its Limited Use requirements.

6. Who receives data and where it is processed

Only the following parties receive data through the App.

Recipient	What they receive	Why
The Organization that invited you	Your health data and the data needed to link it to you in its system	You choose to share it when you connect; the Organization's privacy notice applies
Railway	The license-check data in section 4, stored on our behalf in the European Union	Runs our license server under a data processing agreement
Authorities, courts, professional advisers	License-check data, only where needed	When the law requires it, or to establish or defend legal claims
A buyer or successor of Momentum	License-check data	If our business is merged, sold or reorganized; this policy will continue to apply

Apple and Google provide the app stores, Apple Health and Health Connect under their own privacy policies.

International transfers. Our license server is located in the European Union. If license-check data is transferred outside the European Economic Area or the UK, we use safeguards required by law, such as an adequacy decision or the European Commission's Standard Contractual Clauses. Where your health data is stored depends on where the Organization runs its server.

7. Permissions the App asks for

The App asks only for permissions it needs to sync, and you can withdraw each one at any time.

Permission	Platform	Why	How to withdraw
Read access to health data types	iOS (Apple Health), Android (Health Connect)	To read the data you agreed to share	iOS: Settings > Health > Data Access & Devices > Open Wearables Connect. Android: Health Connect > App permissions > Open Wearables Connect

Permission	Platform	Why	How to withdraw
Read health data in the background	Android (Health Connect)	To sync without the App being open	Health Connect > App permissions > Open Wearables Connect
Background App Refresh	iOS	To sync without the App being open	Settings > General > Background App Refresh
Camera	iOS, Android	Only to scan the invitation QR code; images are not stored or sent	Phone settings > Apps > Open Wearables Connect > Camera

If you withdraw a health permission, the App stops sending that data type. Data already sent stays with the Organization.

8. Disconnecting and deleting your data

You can disconnect in the App at any time, and this also deletes the data we hold about your installation.

- **In the App:** go to Settings > Disconnect this phone and confirm. The App stops syncing, deletes the connection details and license data stored on your phone, and asks our license server to delete your installation ID. If no other installation is connected under your pseudonymous user ID, the server deletes that ID too. If your phone is offline when you disconnect, the request cannot reach us, and the record is deleted automatically after 30 days without a license check. Our server logs are deleted on their normal 30-day cycle.
- **Without the App:** if you have already uninstalled it, request deletion by emailing privacy@openwearables.io. Because we do not know your name, we may ask for details that help us find the right record, such as the Organization's name and the approximate date you connected.
- **Data held by the Organization:** disconnecting stops new data from being sent, but does not delete data the Organization already holds. To delete it, contact the Organization.

Uninstalling the App deletes the data it stores on your phone. On iOS, the sign-in details for the Organization's server stay in the system Keychain, where no other app can read them, until you install the App again; the App then deletes them when it first starts. Our license records expire 30 days after the last license check.

9. Your rights

You have rights over the data we hold, and we honour them wherever you live; requests about your health data go to the Organization.

EU, EEA, UK and Switzerland. You can ask us to give you access to your data, correct it, delete it, restrict its use, or receive it in a portable format. You can object at any time to processing based on our legitimate interests. You can also complain to a data protection authority. Our lead authority is the President of the Personal Data Protection Office (UODO) in Poland, but you can contact the authority where you live or work.

United States. Depending on your state (for example California, Virginia, Colorado or Connecticut), you may have the right to know what data we hold, to delete or correct it, and to appeal our decision. We do not sell personal data or share it for targeted advertising, so there is nothing to opt out of. We will not treat you differently for using your rights.

Consumer health data (Washington, Nevada and similar laws). These laws have separate rules for consumer health data. As a precaution, we address them in section 10.

Other countries. If you live elsewhere, for example in Canada, Brazil or Australia, you have the rights your local law gives you, and we will respond to them in the same way.

How to make a request. Email privacy@openwearables.io or use the in-app option in section 8. We reply within one month (GDPR) or 45 days (US state laws), and may ask for details that help us find your record. If we cannot match a request to any record, we will tell you.

10. U.S. Consumer Health Data Privacy Policy

This section is a precaution only: the App is designed so that we do not collect consumer health data, and we include it in case the broadest possible reading of some U.S. state laws treats our license-check data as such.

Why this section exists. Some U.S. state laws, such as the Washington My Health My Data Act, Nevada's consumer health data law (SB 370) and the consumer health data provisions of the Connecticut Data Privacy Act, define "consumer health data" very broadly. Under those laws, even data that only shows that a person uses a service connected to a healthcare provider or coach could count. Our license-check data (section 4) contains no health information. Because it is linked to the Organization that invited you, an extremely broad reading could still treat it as showing that you seek health-related services from that Organization. We publish this section as a precaution against that reading. It is not an admission that these laws apply to Momentum.

What this section does not cover. Health data the App reads from Apple Health or Health Connect goes directly from your phone to the Organization, and we never receive it (section 3). For that data, the Organization is responsible, and its own privacy notice, including any consumer health data policy it must publish, applies.

Required disclosures.

Topic	Our practice
Categories of data that could be treated as consumer health data	Only the license-check data in section 4: pseudonymous user ID, installation ID, Organization identifier, platform, App version, IP address and time of each check, to the extent that, linked to an Organization, it could indicate that you seek its services. It contains no health information.
Purposes	Verifying that the App is used under a valid subscription, preventing misuse and keeping our systems secure. We do not use this data for any other purpose, and we never use it to infer anything about your health.
Sources	Collected automatically from the App on your device when it checks the license.
Categories of data shared	None. We do not share this data with third parties.
Third parties and affiliates who receive it	No third parties and no affiliates. Our hosting provider Railway stores the data only on our behalf, as a processor under a written contract. We disclose data to authorities only where the law requires it.
Sale	We do not sell this data, or any other data.
Consent	We collect this data only because it is necessary to provide the App you asked to use. We do not collect it for any other purpose, so no separate consent is requested.
Location and geofencing	We do not collect your location and do not use geofencing. If you allow workout routes in Apple Health, the App sends them only to the Organization (section 3); we never receive them.

11. Security, children, changes and contact

Security. All connections from the App, to the Organization and to our license server, are encrypted with TLS. Data on your phone is kept in the App's private storage, protected by your phone's operating system. Access to our license server is limited to authorized staff. No system is completely secure, so please keep your phone locked and up to date.

Children. The App is not intended for children under 16. A younger person may use it only if invited by an Organization that has obtained consent from a parent or guardian where the law requires it. If you believe a child is using the App without such consent, contact the Organization or us.

Changes. We will update this policy when the App or the law changes, and show the new effective date at the top. If a change materially affects how we handle your data, we will tell you in the App before it takes effect.

Contact.

Momentum Sp. z o.o., Poland, Wrocław (53-659), ul. Gen. Władysława Sikorskiego 26, privacy@openwearables.io.