myHealthHub

Privacy Policy

Effective Date: June 2, 2026 | www.myhh.online

1. Introduction

myHealthHub ("we", "us", "our"), operated by Icontent Kft., provides a multi-sided wearable health data platform available at www.myhh.online (the "Platform"). The Platform aggregates biosensor and wearable device data to deliver actionable health insights across a range of service verticals: individuals, employers and corporate wellness teams, insurers, researchers, medical service providers, and food delivery operators.

This Privacy Policy explains how we collect, use, store, share, and protect personal data — including health and biometric data — across all of these service verticals. We are committed to privacy-by-design, explicit consent-based data architecture, and full compliance with the General Data Protection Regulation (GDPR) and applicable Hungarian and EU data protection law.

By using the Platform, you acknowledge that you have read and understood this Privacy Policy.

2. Who We Are (Data Controller)

The Platform is operated by Icontent Kft., a company registered in Hungary, EU. For the purposes of GDPR, myHealthHub acts as:

- Data Controller — for data collected directly from individuals, employers, insurers, researchers, medical providers, and food delivery partners who register on the Platform.
- Data Processor — for employee or end-user health data processed on behalf of an organisational client (the Controller), pursuant to a Data Processing Agreement (DPA).

Contact for privacy matters:

Email: privacy@myhh.online

Website: https://www.myhh.online

Address: Hungary, European Union

3. Platform Services and User Categories

myHealthHub serves the following user groups, each with distinct data processing contexts:

3.1 Individuals

Individual users connect their personal wearable devices and biosensors to gain a unified view of their physical condition. The Platform delivers personalized insights, early risk detection, lifestyle recommendations, progress tracking, and full data ownership and control tools. Individual users are always the primary data subject and retain full control over what data they share, and with whom.

3.2 Employers & Corporate Wellness Teams

Employers and team leaders access anonymised, aggregated workforce wellbeing insights — including stress indicators, recovery trends, and burnout risk — derived from consenting employees' wearable data. No individual-level health data is ever disclosed to employers. All employer dashboards apply k-anonymity (minimum group size: 5 members).

3.3 Insurers

Insurance providers access population-level wellness analytics, predictive risk scoring, personalised wellness programme outputs, and fraud/claim validation tools. All insurer-facing data is anonymised and aggregated. Individual health data is never shared with insurers in identifiable form without the explicit, separate consent of the data subject.

3.4 Researchers

Academic and clinical researchers access standardised, anonymised, real-world biosensor datasets for longitudinal studies, observational research, and health innovation in areas such as aging, lifestyle, and chronic disease. All research datasets are GDPR-compliant, consent-gated, and stripped of direct identifiers prior to access.

3.5 Medical Service Providers

Clinics, hospitals, and care teams integrate wearable data into patient care workflows to support continuous monitoring, early intervention, personalised treatment planning, and preventive care. Medical providers access patient data under a formal Data Processing Agreement and only with patient consent.

3.6 Food Delivery Operators

Food delivery partners receive anonymised, aggregate nutrition and metabolic trend data to enable health-aware menu tagging, personalised meal recommendations, and population-level nutrition analytics. No individual user's identifiable health data is shared with food delivery partners without explicit, separate user consent.

---

4. Personal Data We Collect

4.1 Account & Identity Data

When registering on the Platform (as any user type), we collect:

- Full name and email address
- Organisation name and role (for business accounts)
- Account credentials (passwords stored in hashed form only)
- Billing information (processed securely by our payment provider; we do not store raw payment card data)

4.2 Health & Biometric Data

With explicit consent, we collect the following data from connected wearable devices and biosensors:

- Heart rate and heart rate variability (HRV)
- Recovery scores and readiness metrics (e.g. WHOOP, Polar)
- Activity data: steps, movement intensity, caloric estimates
- Sleep duration, stages, and quality metrics
- Blood glucose and continuous glucose monitoring (CGM) data (e.g. Sibionics)
- Stress scores derived from biometric signals
- Body composition metrics where provided by the device

Health and biometric data constitutes "special category" data under GDPR Article 9 and is processed only with explicit consent (Art. 9(2)(a)) or, where applicable, for research purposes (Art. 9(2)(j)) under appropriate safeguards.

4.3 Calendar & Meeting Data

With explicit consent, the Platform may connect to Google Calendar or Microsoft 365 to retrieve calendar and meeting load data. This is used solely for wellbeing correlation analysis (e.g. meeting density vs. stress indicators) within the employer wellness vertical. This data is not shared with third parties.

4.4 Nutrition & Food Preference Data

Within the food delivery vertical, the Platform may process meal preference, dietary restriction, and nutritional intake data — linked to metabolic and biometric data — to generate personalised meal recommendations. This data is processed only with user consent and is not shared with food delivery partners in identifiable form.

4.5 Usage & Technical Data

We automatically collect technical data when you use the Platform:

- IP address, browser type and version, device type and operating system
- Pages visited, session duration, and interaction logs
- Error and crash reports

This data is collected to maintain, secure, and improve the Platform.

4.6 Data You Provide Directly

You may also provide data through support requests, survey responses, feedback forms, or voice-based wellbeing check-ins recorded via the Platform (transcribed using speech-to-text technology). Voice recordings are processed only with consent and are not retained beyond the transcription process unless you explicitly request otherwise.

---

5. Legal Basis for Processing

We process personal data only where we have a valid legal basis under GDPR. The applicable legal bases vary by processing activity:

- Consent (Art. 6(1)(a) and Art. 9(2)(a)): Explicit, freely given, informed consent is required before any biometric or health data is collected. Consent for special

category data is always obtained separately and in writing. Consent may be withdrawn at any time without affecting the lawfulness of prior processing.
- Contract (Art. 6(1)(b)): Processing necessary to provide the Platform services to registered users and organisational clients.
- Legitimate Interests (Art. 6(1)(f)): Platform security, fraud prevention, and service improvement — where these interests are not overridden by your rights.
- Legal Obligation (Art. 6(1)(c)): Where required to comply with applicable Hungarian or EU law.
- Research / Public Interest (Art. 9(2)(j)): For anonymised research datasets, subject to appropriate technical and organisational safeguards (pseudonymisation, access controls, ethical review).

---

6. 6. How We Use Your Data

6.1 Across All Service Verticals

- Providing, operating, and securing the Platform
- Authenticating users and managing accounts
- Communicating service updates, security notices, and support responses
- Compliance with legal obligations and regulatory requirements
- Fraud detection, abuse prevention, and platform integrity
- Improving and developing Platform features

6.2 Individual Users

- Generating unified health dashboards from connected wearable devices
- Producing AI-powered personalised insights, risk signals, and lifestyle recommendations
- Visualising long-term health trends and progress tracking
- Enabling users to control, export, and delete their data

6.3 Employer / Corporate Wellness

- Aggregating and anonymising employee health metrics for team-level reporting
- Generating workforce wellbeing insights: stress, recovery, burnout risk
- Correlating meeting load data with wellbeing indicators
- Supporting HR and ESG reporting on workforce health metrics

6.4 Insurers

- Producing anonymised population health and risk analytics
- Supporting predictive risk scoring for prevention programme design
- Enabling personalised wellness programme delivery to consenting members
- Providing biosensor-backed claim validation data (with member consent)

6.5 Researchers

- Providing access to anonymised, standardised, longitudinal biosensor datasets
- Supporting observational and interventional health research
- Enabling multi-source data harmonisation for cross-device studies

- Facilitating collaboration between research institutions and healthcare organisations

6.6 Medical Service Providers

- Enabling continuous patient monitoring via real-time biometric data
- Supporting AI-driven treatment personalisation based on objective lifestyle data
- Providing clinicians with consolidated patient biosensor data
- Facilitating preventive care by identifying early physiological risk patterns

6.7 Food Delivery Operators

- Generating anonymised population-level nutrition and metabolic trend analytics
- Enabling health-aware menu classification and tagging
- Supporting personalised meal and supplement recommendations (with user consent)
- Predicting individual metabolic responses to food items (with user consent)

We do not use personal health data for targeted advertising. We do not sell your data to any third party.

---

7. Data Sharing & Disclosure

7.1 Organisational Clients (Employers, Insurers, Medical Providers, Food Operators)

Organisational clients receive only anonymised, aggregated insights relevant to their service vertical. No individual end-user's identifiable health data is disclosed to any organisational client without that user's explicit, separate consent. All organisational client access is governed by a Data Processing Agreement.

7.2 Wearable & Integration Partners

To retrieve health data, the Platform integrates with third-party APIs via OAuth2. Access tokens are stored securely and scoped to read-only health data. Current integrations include:

- WHOOP API
- Polar AccessLink v4
- Fitbit / Google Health API
- Sibionics CGM API
- Google Calendar API
- Microsoft Graph API (MS365 Calendar)

Each integration requires explicit user authorisation. Data is not transferred to these providers beyond what is technically necessary to retrieve your health data.

7.3 Research Partners

Anonymised, aggregated research datasets may be shared with academic institutions, healthcare organisations, and research collaborators. All research data sharing is governed by data sharing agreements that prohibit re-identification and require ethical oversight.

7.4 Service Providers (Processors)

We engage trusted third-party processors under GDPR-compliant data processing agreements:

- Heroku (Salesforce) — cloud hosting and application infrastructure
- Backblaze B2 — cloud document storage
- GitHub — source code management (no personal data stored)
- Email service providers — transactional and account notifications

All processors are prohibited from using your data for their own purposes.

7.5 Legal Requirements

We may disclose personal data to law enforcement, courts, or regulatory authorities where required by law, or to protect the rights, property, or safety of myHealthHub, our users, or the public.

7.6 Business Transfers

In the event of a merger, acquisition, or asset sale, personal data may be transferred to the acquiring entity. Affected users will be notified in advance, and the acquirer will be required to honour this Privacy Policy.

---

8. Anonymisation & Privacy Architecture

Privacy protection is built into the technical architecture of the Platform:

- Pseudonymisation: Employee and end-user health data is pseudonymised at the point of ingestion. Direct identifiers are replaced with pseudonymous IDs before any processing for analytics or reporting.
- K-anonymity: Employer-facing dashboards apply a minimum group size of 5 individuals. No aggregate metric is displayed if fewer than 5 data subjects contribute to it.
- Differential privacy techniques: Applied where feasible for population analytics shared with insurers, researchers, and food delivery operators, to prevent individual re-identification.
- Role-based access controls: Platform users only access data relevant to their user role. Employers cannot access individual employee data. Insurers cannot access individual member data.
- Data minimisation: We collect only the data necessary for the specific service being delivered.

---

9. Data Retention

- Account data: retained for the duration of the account plus 2 years after closure
- Individual and employee health data: retained for a maximum of 24 months from collection, or until consent is withdrawn — whichever is earlier
- Medical patient data: retained in accordance with applicable healthcare record retention obligations and the terms of the Data Processing Agreement with the medical provider
- Research datasets (anonymised): may be retained indefinitely as they cannot be linked to individuals
- Usage and technical logs: retained for up to 12 months

- Voice recordings and transcripts: deleted within 30 days of transcription unless explicitly retained by user request

You may request early deletion of your data at any time (see Section 10).

---

10. Your Data Protection Rights

As a data subject under GDPR, you have the following rights, exercisable free of charge:

- Right of Access (Art. 15): Request a copy of the personal data we hold about you.
- Right to Rectification (Art. 16): Request correction of inaccurate or incomplete data.
- Right to Erasure (Art. 17): Request deletion of your personal data.
- Right to Restriction (Art. 18): Request that we restrict processing of your data.
- Right to Data Portability (Art. 20): Receive your data in a structured, machine-readable format.
- Right to Object (Art. 21): Object to processing based on legitimate interests.
- Right to Withdraw Consent (Art. 7(3)): Withdraw consent for health data processing at any time, without affecting the lawfulness of prior processing.
- Right to Lodge a Complaint: File a complaint with the Hungarian supervisory authority (NAIH) or with the supervisory authority in your country of residence.

To exercise any of these rights, contact us at: privacy@myhh.online

We will respond within 30 days. Identity verification may be required before fulfilling your request. For research participants, exercise of certain rights (e.g. erasure) may be limited where data has already been fully anonymised.

---

11. Data Security

We implement appropriate technical and organisational measures to protect personal data:

- All data in transit is encrypted using HTTPS/TLS
- Passwords are stored using strong cryptographic hashing (never in plaintext)
- OAuth2 access tokens are stored in encrypted fields and rotated regularly
- Health data is pseudonymised at the point of ingestion
- Access to personal data is restricted on a strict need-to-know basis
- Regular security reviews, dependency audits, and penetration testing
- Separate credentials and infrastructure per deployment environment (development, staging, production)

In the event of a personal data breach, we will notify affected users and the relevant supervisory authority (NAIH) within 72 hours, in accordance with GDPR Article 33.

---

12. International Data Transfers

myHealthHub is based in Hungary (EU) and primarily processes data within the European Economic Area (EEA). Where data is transferred outside the EEA (e.g. to API partners), we ensure appropriate safeguards are in place:

- Standard Contractual Clauses (SCCs) approved by the European Commission
- Adequacy decisions where applicable

Wearable API integrations (WHOOP, Polar, Fitbit, Google, etc.) involve data exchange with servers that may be located outside the EEA. By authorising these integrations, you consent to the associated cross-border data flows, which are technically necessary to retrieve your health data.

---

13. Cookies & Tracking Technologies

- Essential cookies: Required for login sessions, CSRF protection, and Platform security. Cannot be disabled.
- Analytics cookies: Used to understand Platform usage patterns and improve user experience. Set only with your consent.

You can manage cookie preferences in your browser settings. Disabling non-essential cookies does not affect core Platform functionality.

---

14. Children's Privacy

The Platform is intended for adult users (18+) in professional, clinical, or consumer health contexts. We do not knowingly collect data from individuals under the age of 18. If we become aware that a minor has provided personal data, we will delete it promptly.

---

15. Changes to This Privacy Policy

We may update this Privacy Policy to reflect changes in our services, technology, or legal requirements. When we make material changes, we will:

- Update the Effective Date at the top of this document
- Notify registered users by email or in-app notification
- Obtain fresh consent where required by law

Continued use of the Platform after changes take effect constitutes acceptance of the revised Policy.

---

16. Contact Us

For any questions, concerns, or requests relating to this Privacy Policy or the handling of your personal data:

myHealthHub — Privacy Contact

Email: privacy@myhh.online

Website: https://www.myhh.online

Operator: Icontent Kft., Hungary, European Union

You also have the right to contact the Hungarian data protection supervisory authority:

NAIH — Nemzeti Adatvédelmi és Információszabadság Hatóság

Website: www.naih.hu | Email: ugyfelszolgalat@naih.hu
