Zack Health: Data Privacy & GDPR Policy

Effective Date: January 1st, 2025
Last Updated: August 3rd, 2025

We may update this policy to reflect changes in law or our operational practices. Updates will be posted here with an updated date.

Operator Information

Company Name: Zack Health ApS
VAT Number: DK45311597
Address: Banebrinken 99, 2400 Copenhagen NV, Denmark
Email: hey@zackhealth.com

"Zack Health", "we", "us" and "our" refer to Zack Health ApS. "You", "your", or "user" refers to the individual accessing or using our services.

Introduction

At Zack Health, protecting your privacy and personal data is our highest priority. This policy explains how we collect, process, store, and share your data in compliance with the General Data Protection Regulation (GDPR) and applicable law. By using our services, you agree to the terms outlined in this policy.

Why You Can Trust Us With Your Data

At Zack Health, your data is not our product. We don't sell, license, or share your individual health data. Our mission is to serve your health. Any internal improvements or research we do with data are built on privacy by design, always using de-identified, anonymized, or aggregated data.

You stay in control. We build our systems to earn your trust – not to exploit it.

Role of Zack Health

Zack Health acts as the data controller for personal data collected and processed in connection with providing our services.

In certain cases, we rely on third-party providers (e.g. laboratories, hosting, analytics). These providers act as data processors under our instruction and are bound by GDPR-compliant Data Processing Agreements (DPAs).

Zack Health does not act as a joint controller with employers or laboratories, as no identifiable personal data is shared with them.

Principles of Data Processing

We adhere to the following GDPR principles:

- Lawfulness, Fairness, and Transparency
- Purpose Limitation

- Data Minimization
- Accuracy
- Storage Limitation
- Integrity and Confidentiality (Security)

Data We Collect

- **Personal Information:** Name, email, and contact details
- **Health Data:** Lab results, health check measurements, self-reported health information
- **Lifestyle Data:** Diet, exercise, sleep, and related behaviors
- **Technical Data:** We use cookie-free analytics to understand basic usage patterns and improve our services. This may include non-identifiable information such as device type, browser type, and general usage data. We do not use third-party tracking cookies or advertising trackers.

Data is stored securely in systems with strict access controls. Our storage providers comply with GDPR. Laboratories receive only de-identified biological samples – no personal identifiers are included.

Purposes of Processing

We process your personal data to:

- Deliver personalized health assessments and recommendations
- Provide technical support and improve service functionality
- Conduct internal analysis to optimize services and technology
- Use anonymized or pseudonymized data for research, development, and algorithmic improvements
- Share fully aggregated and anonymized reports with employers (only when health checks are employer-sponsored, at least 20 individuals have participated, and no individual can be identified)
- Comply with legal and regulatory obligations

Use of AI & Health Models

Zack Health uses large language models (LLMs) in limited ways today – for example, to help generate draft content such as health report summaries or explanations. These outputs are always reviewed and approved by qualified humans before being shown to users. No AI-generated content is used to make decisions about your health without human oversight.

When implemented:

- Models will not make automated decisions with legal or similarly significant effects without human involvement
- All AI-generated outputs will remain subject to human review
- We will maintain transparency about how data is used to train and validate models
- All use of AI is developed and operated in accordance with the EU AI Act and other applicable regulations

Legal Bases

Our data processing is based on the following legal bases under GDPR:

- Consent (Art. 6(1)(a)) – For non-sensitive data where consent is required
- Explicit Consent (Art. 9(2)(a)) – For processing special categories of data, including health

- Contractual Necessity (Art. 6(1)(b)) – To provide services you have requested
- Legal Obligation (Art. 6(1)(c)) – For compliance with legal obligations
- Legitimate Interests (Art. 6(1)(f)) – For internal use cases like service improvement or fraud prevention, provided your rights are not overridden

Consent

We collect explicit consent for processing your sensitive health data, as required under GDPR Article 9(2)(a). This consent is obtained when you purchase or sign up for a health check or test kit, or during registration.

You may withdraw your consent at any time by contacting us at hey@zackhealth.com. Withdrawal may affect your access to certain services.

Data Sharing

We share data only under strict safeguards and in the following cases:

Third-Party Processors

We work with carefully selected third parties, including laboratories (who receive de-identified samples only), IT infrastructure providers, analytics tools, and customer support systems. All third parties operate under GDPR-compliant Data Processing Agreements (DPAs).

We may use fully anonymized and aggregated data to support internal research, product development, or to generate insights that help improve health outcomes at scale.

No decisions are made solely by automated systems that significantly affect you without human involvement.

Employers

When health checks are sponsored by your employer, Zack Health provides fully aggregated, anonymized, non-personal reports back to the company. These reports help employers understand broad health trends in their organization so they can invest in the right wellness programs and support.

Here's how we protect you:

- Employers never see individual data, results, or names
- Reports require a minimum of 20 participants and are structured to prevent re-identification
- Only group-level insights are shared, and only when these meet our strict anonymity thresholds

Research & Healthcare Institutions

We may share anonymized or pseudonymized data with trusted institutions for research or public health purposes.

International Transfers

If personal data is transferred outside the EU/EEA (e.g. through cloud hosting or analytics tools), we apply appropriate safeguards, including:

- Standard Contractual Clauses (SCCs)

- Adequacy decisions (where applicable)
- Other approved mechanisms under GDPR

Data Retention

We retain your personal data for up to 60 months after your last activity, unless we are legally required to retain it longer (e.g. for tax or compliance purposes). After this period, your data is either anonymized or securely deleted.

If you actively use our services, we retain your data as long as needed to deliver them. Once your relationship with Zack Health ends, we minimize or delete your data unless we are required by law or have a legitimate reason to retain it.

User Control Over Data Retention:

- You may delete your data or reports at any time, unless legal obligations require retention
- You may delete your entire profile unless required otherwise by law
- If you are inactive for 60 months, your data will be deleted. We will notify you 30 days in advance
- If your employer's agreement with Zack Health ends, your data will be deleted unless legal obligations require otherwise

Data Security

We protect your data through:

- Encryption (in transit and at rest)
- Role-based access control
- Security monitoring and regular audits
- Mandatory staff training on data handling

In the event of a personal data breach, we will notify the Danish Data Protection Agency (Datatilsynet) within 72 hours, and affected users if required.

Your Rights

As a data subject under GDPR, you have the right to:

- Access your personal data
- Correct inaccurate or incomplete data
- Delete your data ("right to be forgotten")
- Restrict or object to certain types of processing
- Request data portability
- Withdraw consent at any time
- File a complaint with your local supervisory authority (Datatilsynet)

To exercise your rights, contact us at hey@zackhealth.com. We will respond to all valid requests within 30 days.

Cookies

We do not use third-party tracking or advertising cookies, because of your privacy.

Our website uses only:

- Essential cookies – for core website functionality and security.
- Cookie-free analytics – to understand basic usage patterns (e.g. page views, device type). These analytics do not rely on cookies, do not track individuals across websites, and cannot identify you.

Because our analytics are cookie-free and non-personal, no consent banner is required.

Automated Decision-Making

We do not make decisions based solely on automated processing that produce legal or similarly significant effects.

Where personalization or recommendations are provided by AI, these outputs are always subject to human oversight.

Children's Data

Our services are not intended for individuals under the age of 16. We do not knowingly collect or process personal data from minors. If we become aware that personal data from a minor has been collected, we will delete it without delay.

Contact

For any privacy-related questions or to exercise your data rights, contact us:

Email: hey@zackhealth.com