

PRIVACY POLICY

Nightingale Project | Innovation in Medicine GbR

Effective Date: 16 March 2026 | Version 1.0

Applies to: www.nightingaleheart.com

1. Introduction and Data Controller

Welcome to the Nightingale Project. We take the protection of your personal data seriously. This Privacy Policy explains what information we collect, why we collect it, and how it is used when you visit our website at www.nightingaleheart.com and use our heart health awareness tool.

Data Controller: Innovation in Medicine GbR (Nightingale Project), Nikolaus-Otto-Strasse 6, 55129 Mainz, Germany

Email: info@nightingaleheart.com

Website: www.nightingaleheart.com

This policy complies with:

- Regulation (EU) 2016/679 — General Data Protection Regulation (GDPR)
- German Federal Data Protection Act (Bundesdatenschutzgesetz — BDSG)
- German Telemedia Act (Telemediengesetz — TMG)

2. Personal Data We Collect

2.1 Data You Provide Directly

When you contact us or correspond with us, we may collect your name and email address. This applies only when you actively reach out to us — for example, via the contact form or by emailing info@nightingaleheart.com.

2.2 Data Collected Automatically

When you visit our website, we automatically collect certain technical information:

- IP address and approximate geographic location
- Browser type, version, and operating system

- Pages visited, time spent, and navigation data
- Device type and screen resolution
- Cookies and similar tracking technologies (see Section 11)

2.3 Our Heart Health Awareness Tool — No Data Retained

Our heart health tool asks you a short questionnaire and provides a general, personalised overview of your heart health based on your answers. This tool is designed with privacy by default:

- No health information you enter is stored, logged, or transmitted to any server or third party.
- All processing happens temporarily within your active session only.
- When your session ends, all inputs and outputs are permanently discarded.
- We do not build profiles, retain results, or link questionnaire responses to any individual.

Because no personal or health data is retained beyond your session, there is no health data subject to long-term processing under GDPR Article 9.

3. Legal Basis for Processing

We process personal data on the following legal grounds under GDPR:

- **For optional analytics and error reporting where you have given consent via our cookie/consent tool. You may withdraw consent at any time.** Consent (Article 6(1)(a)):
- **For website security, fraud prevention, and basic analytics to understand how our website is used.** Legitimate Interests (Article 6(1)(f)):
- **Where required to comply with applicable German or EU law.** Legal Obligation (Article 6(1)(c)):
- **For essential in-session processing when you use our heart health tool.** Contractual Necessity (Article 6(1)(b)):

4. Our Heart Health Awareness Tool

4.1 What It Does

Nightingale Heart tools presents you with a short questionnaire and, based on your answers, provides a general indication of your heart health. It is a self-serve awareness tool — similar in

nature to an online health calculator or symptom checker — intended to give you a starting point for thinking about your cardiovascular wellbeing.

4.2 What It Is Not

This tool does not constitute medical advice, a clinical assessment, or a diagnosis. It is not a certified medical device. Results are for general informational purposes only and should not be acted upon without consulting a qualified healthcare professional. If you have any concerns about your heart health, please speak with your doctor.

4.3 AI and Transparency

The tool uses AI to generate your personalised overview. We are transparent that AI is involved in this process. The output reflects patterns in the information you provide and is not reviewed or verified by a medical professional. No automated decision with legal or clinical consequences is ever made about you.

4.4 No Automated Decision-Making with Significant Effects

Under GDPR Article 22, you have rights concerning automated decision-making. Our tool produces general informational outputs only. It does not make decisions that produce legal effects or similarly significant consequences for you.

5. How We Use Your Data

We use personal data only for the purposes for which it was collected:

- Responding to enquiries and correspondence
- Operating and improving our website
- Website security, fraud prevention, and technical operations
- Anonymous, aggregated analytics to understand usage patterns (where consent is given)
- Compliance with applicable legal obligations

We do not sell your personal data to third parties. We do not use your data for targeted advertising. We do not use health questionnaire inputs for any purpose beyond your immediate session.

6. Data Sharing and Recipients

We do not sell personal data. We may share data with:

- **Hosting, analytics, and infrastructure providers who process data on our behalf under Data Processing Agreements (DPAs) in accordance with GDPR Article 28.**Service Providers:
- **Where required by applicable law, court order, or regulatory obligation.**Legal Authorities:

All processors are contractually required to implement appropriate security measures and process data only as instructed by us.

7. International Data Transfers

Our primary operations are based in Germany within the European Economic Area (EEA). Where any data is transferred outside the EEA — for example, to cloud infrastructure providers — we ensure appropriate safeguards are in place, including Standard Contractual Clauses (SCCs) approved by the European Commission or applicable adequacy decisions.

8. Data Retention

We retain personal data only for as long as necessary:

- Heart health tool inputs and outputs: Not retained. Discarded at end of session.
- Website analytics data: 13 months from collection.
- Contact and correspondence data: 3 years from last contact.
- Legal and compliance records: As required by law (typically 6–10 years).

When data is no longer required, it is securely deleted or anonymised.

9. Your Rights Under GDPR

You have the following rights regarding your personal data:

- **Request a copy of all personal data we hold about you.**Right of Access (Article 15):
- **Request correction of inaccurate or incomplete data.**Right to Rectification (Article 16):
- **Request deletion of your data where there is no compelling reason for continued processing.**Right to Erasure (Article 17):
- **Request that we limit how we use your data.**Right to Restriction (Article 18):

- **Receive your data in a structured, machine-readable format.** Right to Data Portability (Article 20):
- **Object to processing based on legitimate interests.** Right to Object (Article 21):
- **Withdraw consent at any time without affecting the lawfulness of prior processing.** Right to Withdraw Consent (Article 7(3)):

To exercise any of these rights, contact us at info@nightingaleheart.com. We will respond within 30 days. No fee will be charged.

10. Data Security

We implement appropriate technical and organisational measures to protect your personal data in accordance with GDPR Article 32, including:

- Encryption of data in transit (TLS/SSL)
- Access controls and role-based permissions
- Regular security assessments
- Staff training on data protection
- Incident response procedures

In the event of a personal data breach posing risk to your rights and freedoms, we will notify the relevant supervisory authority within 72 hours and affected individuals without undue delay, as required by GDPR Articles 33–34.

11. Cookies and Consent Tool

We use cookies and similar technologies on our website. When you first visit, you will see our consent popup, which allows you to:

- Accept essential cookies only — required for the website and heart health tool to function. No personal data is retained from tool use.
- Optionally consent to anonymous usage analytics — aggregated, non-identifiable data on how features are used. No health content is included.
- Optionally consent to crash and error reporting — technical logs to help us fix bugs, stripped of session content before transmission.

You can withdraw or update your cookie preferences at any time via the consent settings in the website footer, or by contacting us at info@nightingaleheart.com.

For full details on the cookies we use, please refer to our Cookie Policy at www.nightingaleheart.com/cookies.

12. Children's Data

Our services are not directed at children under the age of 16. We do not knowingly collect personal data from children under 16 without verifiable parental consent. If you believe we have inadvertently collected data from a child, please contact us immediately at info@nightingaleheart.com and we will delete it promptly.

13. Supervisory Authority and Complaints

You have the right to lodge a complaint with a data protection supervisory authority at any time. The competent authority for the Nightingale Project is:

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz (LfDI)

Hinterer Bleiche 34, 55116 Mainz, Germany

Website: www.datenschutz.rlp.de

Email: poststelle@lfdi.rlp.de

You may also contact the supervisory authority in your EU member state of habitual residence or place of work.

14. Changes to This Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, technology, or legal requirements. We will notify you of significant changes by posting a prominent notice on our website and updating the effective date above. Where required by law, we will seek renewed consent.

Continued use of our services after changes constitutes acceptance of the updated policy.

15. Contact Us

For any questions, concerns, or requests regarding this Privacy Policy or your personal data, please contact:

Nightingale Project | Innovation in Medicine GbR

Nikolaus-Otto-Strasse 6, 55129 Mainz, Germany

Email: info@nightingaleheart.com

Website: www.nightingaleheart.com

We aim to respond to all requests within 30 days.

This Privacy Policy was last reviewed and approved on 16 March 2026.