GDPR Compliance Statement for Paindrainer AB

Effective Date: 2025-11-10

At **Paindrainer AB**, we are fully committed to safeguarding the privacy and personal data of our users in compliance with the **General Data Protection Regulation (EU) 2016/679 (GDPR)** and applicable national data protection laws.

This statement outlines our compliance posture and key principles governing the processing of personal data across our services and our website, www.paindrainer.com.

1. Data Controller and Contact Information

Paindrainer AB, Org. no. 559156–5196, headquartered at Medicon Village, 223 81 Lund, Sweden, is the data controller under Article 4(7) GDPR.

For inquiries:

- General: **info@paindrainer.com**
- Data Privacy Officer (DPO): **dpo@paindrainer.com**

2. Lawful Basis for Processing

We process personal data on the following legal bases:

- **Performance of a contract** (Art. 6(1)(b)) – for providing services to users.
- **Consent** (Art. 6(1)(a) and Art. 9(2)(a)) – especially for processing special categories of personal data (e.g., health data).
- **Legitimate interests** (Art. 6(1)(f)) – such as improving our services and system monitoring.
- **Legal obligations** (e.g., bookkeeping laws).

3. Categories of Personal Data Processed

We process:

- Identifiers: name, address, email, phone number, date of birth.
- Financial details: billing and card information.
- Health-related data: diagnostic inputs, pain logs, activity levels.
- Technical metadata: IP addresses, device data, and usage patterns (website only).
- Employment and organizational affiliation (where applicable).

4. Special Categories of Data

Health data is processed only with **explicit user consent**, in accordance with Article 9(2)(a) GDPR. Such data is essential for the functionality of the Paindrainer service, particularly when prescribed by a healthcare provider.

5. Data Subject Rights

Users have the right to:

- Access, rectify, or erase their data.
- Restrict or object to processing.
- Data portability.
- Withdraw consent at any time without affecting prior lawful processing.
- Lodge complaints with the Swedish Authority for Privacy Protection (IMY).

Requests can be submitted to: **info@paindrainer.com**

6. Data Transfers Outside the EU/EEA

Where data is transferred outside the EU/EEA (e.g., to the USA), we ensure appropriate safeguards are in place, such as **Standard Contractual Clauses (SCCs)** approved by the European Commission, in compliance with Chapter V GDPR.

7. Data Retention

- Personal data is retained as long as necessary to fulfill the stated purposes.
- Health and account data is retained for up to six (6) months after account closure, unless required longer by law or for clinical research (up to ten (10) years).
- Aggregated and anonymized data may be retained for research and service development.

8. Data Security

Paindrainer AB is committed to maintaining a high level of security to protect the personal data of our users. We implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks associated with our data processing activities.

These measures include, but are not limited to:

- Role-based access controls to restrict data access to authorized personnel only.
- Encryption of data in transit and at rest.
- Secure infrastructure hosting and regular vulnerability assessments.
- Staff training on data protection and confidentiality obligations.
- Ongoing monitoring of systems to detect and prevent unauthorized access or misuse.
- In addition, Paindrainer AB has successfully completed a **SOC 2 Type II audit** covering the **Security**, **Availability**, and **Confidentiality** trust service criteria. This independent third-party attestation demonstrates that our controls are not only well-designed but have been effectively operated over time to protect user data from unauthorized access, ensure continuous availability of our services, and maintain strict confidentiality standards.
- Our SOC 2 compliance reinforces our alignment with GDPR requirements, providing additional assurance to users and partners regarding the integrity and reliability of our data protection practices.

9. Third Parties and Processors

Data may be shared with service providers, clinics, and authorized partners under strict data processing agreements. All third parties are contractually bound to adhere to GDPR-compliant data protection standards.

10. Updates

We review and update our data protection practices regularly. Significant changes to our privacy policy will be communicated via the website, app notifications, or email.

Elin Algotsson
Digitally signed by Elin Algotsson
Date: 2025.11.10 13:08:52 +01'00'

Elin Algotsson, Data Privacy Officer

Erik Frick
Elektroniskt undertecknad av Erik Frick
Datum: 2025.11.10 13:13:13 +01'00'

Erik Frick, CEO