Data privacy at nilo

Get in touch

hi@nilohealth.com or +49 302 178 2152

Legal & Data Responsibility

- nilo and its customers act as independent controllers under Article 4 No. 7 GDPR.
- Employees register directly to use nilo services and enter into their own contractual relationship with nilo.
- nilo is independently responsible for processing personal data of employees using nilo

Security & infrastructure

- Data is protected by advanced encryption algorithms.
- nilo is SSL certified and operates exclusively over SSL-encrypted connections.
- Annual penetration tests ensure top-tier security.
- We operate with strict internal security policies, i.a. password length requirements, Multi-Factor Authentication (MFA) and VPN use for accessing user data.

Confidentiality

- All communication between employees and nilo experts (or in group sessions) is strictly confidential.
- nilo experts operate under strict confidentiality guidelines and have signed confidentiality agreements. They do not share any confidential information with nilo or third parties.
- Only aggregated usage data (e.g. participation rates) may be shared with the customer.

Offboarding & integration

- To ensure secure access and offboarding, nilo sends regular verification emails to company-provided addresses.
  If verification is not possible, platform access is denied.
- An optional Personio-integration is available to support automated offboarding

GDPR & compliance

- nilo is fully GDPR compliant.
- All data is processed within Europe and stored securely on servers located in Germany.
- nilo provides a Confirmation of GDPR Compliance upon request (accessible to third parties).

Data protection at nilo

- Terms of use end user
- Privacy policy end user
- Terms & conditions for customers
- Technical & organizational measures (TOMs)
- Confirmation of GDPR compliance

Your partner for mental health at work