Privacy Policy

We take the protection of your personal data very seriously. Here you will find transparent information on how we handle your data.

Last updated: July 2026

1. Controller and Data Protection Officer

The controller within the meaning of the General Data Protection Regulation (GDPR) and the German Federal Data Protection Act (BDSG) is:

Company: SitzFritz Health GmbH
Address: Rheinwerkallee 6, 53227 Bonn, Germany
Represented by: Managing Directors: Pascal Harth & Niklas Best
Commercial Register: Amtsgericht Bonn, HRB 30845
Email: privacy@sitzfritz.de

A statutory Data Protection Officer (DPO) has not been appointed, as the legal requirements under Art. 37 GDPR / § 38 BDSG are not met. Should this change, we will publish the relevant information here.

2. Legal Bases for Data Processing

We process personal data exclusively in accordance with the GDPR, the BDSG and other applicable data protection legislation. The legal bases for processing are in particular:

Art. 6(1) a) GDPR - Consent: e.g. optional cloud synchronisation, AI webcam posture analysis, newsletter subscription, gamification leaderboards, website analytics.

Art. 6(1) b) GDPR - Performance of a contract: e.g. provision of the application, account and sign-in management, licence management, payment processing.

Art. 6(1) c) GDPR - Legal obligation: e.g. statutory retention obligations under tax law.

Art. 6(1) f) GDPR - Legitimate interests: e.g. IT security, prevention of abuse, licence verification.

Obligation to provide data: Providing your email address and name is required to conclude a user agreement and create an account. Without this data, we are unable to provide our services. The provision of data for cloud synchronisation or the webcam feature is entirely voluntary; declining to do so has no effect on your ability to use the core local application.

3. Categories of Personal Data Processed

Depending on the scope of use and the subject matter of the agreement, we process the following categories of data:

a) Basic and contact data: Name, email address, postal address (for paid subscriptions / billing address).

b) Account and authentication data: Username, password (stored in encrypted form), session tokens, FIDO/certificate-related data (where applicable).

c) Usage and telemetry data: IP address (for server requests), user agent, event logs, timestamps and session duration, licence verification requests (technically necessary data only).

d) Payment and billing data: Billing address, payment method, invoice number, tax-relevant data (VAT ID for B2B).

e) Profile data: Optional profile picture, language setting (if provided by the user).

f) Optional / opt-in data: Webcam images (processed locally only, no upload); gamification statistics (anonymised, with consent only); cloud backup data (with consent only).

g) Support and communication data: Email correspondence, support tickets.

h) Newsletter data: Email address, registration timestamp, IP address at sign-up, double opt-in confirmation status (with consent only).

4. Processing When Using the Software (Desktop App and Cloud Features)

4.1 Installation and Registration

Use of the application requires the creation of a user account (email address or third-party login). This data is processed on the basis of Art. 6 (1) b) GDPR.

4.2 Local Data Storage (Default)

By default, all user data (settings, statistics, posture trends) is stored locally and in encrypted form on the user's device. No data is transferred to our servers unless the user activates the cloud backup feature.

4.3 Local AI / Webcam Posture Analysis (Opt-In)

Posture analysis via webcam is carried out only following the user's explicit consent (Art. 6 (1) (a) GDPR). Image processing takes place exclusively locally in the device's working memory.

- No raw images or video data are transmitted or stored permanently.
- No biometric raw data is transmitted to the provider's servers.
- Posture assessments are generated locally. They are synchronised only if cloud sync is enabled.
- Consent may be withdrawn at any time in the application settings.

B2B Note (co-determination obligation): Before deploying the webcam feature in a business environment, the employer is obliged under Section 87 (1) No. 6 of the German Works Constitution Act (BetrVG) to either conclude a works agreement (Betriebsvereinbarung) or confirm in writing to SitzFritz that no works council or other relevant employee representative body exists. Activating the feature without meeting these preconditions is not permitted. SitzFritz provides template works-agreement texts on request.

4.4 Licence Verification (Phone Home)

To verify licence entitlement, the application connects to the provider's licence servers at least every 30 days. Only technically necessary data is transmitted (user account, timestamp). Legal basis: Art. 6 (1) (b) GDPR.

4.5 Optional Cloud Sync (Opt-In)

At the user's express request, application data is backed up to the SitzFritz cloud (Microsoft Azure, EU data centre). This enables the usage on multiple devices. Legal basis: Art. 6 (1) a) GDPR. Consent may be withdrawn at any time.

4.6 Gamification / Anonymised Leaderboards (Opt-In)

With consent, anonymised usage metrics are transmitted to our servers to generate leaderboards and badges. The following anonymisation structure applies: In the global gamification leaderboard, only anonymised activity points and badge status values are processed; data is displayed only once more than 10 active users are present, to prevent the identification of individual persons. In the company-internal HR dashboard, aggregate values for the company account are calculated and displayed only when at least 10 employees associated with the account are active. Individual evaluations and the identification of individual employees are technically excluded from the product architecture. No public identification of users takes place. Legal basis: Art. 6 (1) (a) GDPR.

4.7 Dynamic Content

When retrieving new content (tips, exercises) from our servers, technically necessary connection data (IP address, timestamp) is transmitted. Legal basis: Art. 6 (1) b) GDPR.

5. Hosting and Infrastructure: Microsoft Azure (Data Processing Agreement)

We host our backend, databases and all cloud services with Microsoft Azure. The provider is:

Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland

Legal basis: Art. 6 (1) (b) GDPR (performance of contract) and Art. 6 (1) (f) GDPR (legitimate interest in secure and reliable infrastructure).

Data location: Germany (Azure region Germany West Central) & France (Azure region France Central). Data is processed and stored within the European Union.

Data Processing Agreement (DPA): We have concluded a Data Processing Agreement with Microsoft pursuant to Art. 28 GDPR. The DPA is available at: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA.

Third-country transfers: Microsoft uses the EU-U.S. Data Privacy Framework, Standard Contractual Clauses (SCCs) and the EU Data Boundary commitment. Further information: https://www.microsoft.com/en-us/trust-center/privacy/european-data-boundary-eudb.

Server log files: When our website is accessed, connection data is processed by the infrastructure for technical reasons. Any access logs are used solely to ensure operation and IT security; IP addresses are truncated or masked and are not combined with other data sources (Art. 6 (1) (f) GDPR).

6. Business Communication and Productivity (Microsoft 365)

For email communication, scheduling and internal collaboration we use Microsoft 365 (Outlook/Exchange Online, Teams, OneDrive/SharePoint). The provider is also Microsoft Ireland Operations Limited.

Purpose: Handling business correspondence with customers, partners and prospective clients; internal organisation.

Data processed: Contact data (name, email address), communication content, metadata (timestamps, IP address) and personal data contained in documents.

Legal basis: Art. 6 (1) (b) GDPR and Art. 6 (1) (f) GDPR.

Data location & DPA: The conditions set out under Section 5 apply. Data storage is arranged primarily in the EU region (EU Data Boundary).

7. Protection against automated requests: Cloudflare Turnstile

To protect our web forms (e.g. contact form, newsletter sign-up, registration) against automated bot requests and spam, we use the Cloudflare Turnstile service. The provider is

Cloudflare, Inc., 101 Townsend St., San Francisco, CA 94107, USA

Cloudflare Turnstile analyses technical browser signals (e.g. HTTP headers, browser properties, network data) to distinguish between human users and automated systems. Cloudflare states that the transmitted data is not used for advertising or profiling purposes.

Cloudflare Turnstile may set functional cookies or LocalStorage entries during bot detection. These are technically necessary and do not require consent (Section 25(2) TDDDG).

Legal basis: Art. 6(1)(f) GDPR (legitimate interest in the security of our website and services).

DPA: Concluded pursuant to Art. 28 GDPR. The DPA is available at: cloudflare.com/cloudflare-customer-dpa.

Third-country transfers: Cloudflare is certified under the EU-U.S. Data Privacy Framework and uses Standard Contractual Clauses (Art. 46(2)© GDPR).

Cloudflare Privacy Policy: cloudflare.com/privacypolicy.

8. Website Analysis

To analyse and optimise our services, we collect anonymised reach and usage statistics following your explicit consent. We record page views as well as anonymous interaction events (e.g. scroll depth, clicks on outbound links and downloads, and technical errors). Processing takes place exclusively on our own infrastructure; no data is transferred to third parties.

- **Storage location:** Azure Table Storage, Region Germany West Central (EU)
- **Data processed:** Event type, hashed IP address (SHA-256 with salt, truncated to 16 characters), user agent, URL path visited, referring page, time on page, language, screen resolution, first-visit flag, anonymous session ID, approximate location (country) derived from the IP address, campaign parameters of the calling URL (utm_*) where present, and an event detail (e.g. scroll depth in percent, outbound link target, file name, error message). The IP address is processed solely to derive the approximate location and to form the hash value, and is not stored in plain text.
- **Legal basis:** Art. 6(1)(a) GDPR (consent)
- **Withdrawal:** At any time via cookie settings, with effect for the future
- **Storage period** 14 months from collection; automated deletion thereafter

9. Payment Processing and Accounting

Within our organisation, personal data is shared only with those departments that require it to fulfil their responsibilities.

9.1 Mollie (Credit Card, SEPA Direct Debit, PayPal, Apple Pay, Google Pay, etc.)

Payment provider: If you opt for a paid service on our website, we process the payment via the payment service provider Mollie. The provider is Mollie B.V., Keizersgracht 126, 1015 CW Amsterdam, Netherlands (hereinafter “Mollie”). The data entered during payment (e.g. name, address, account number, credit card number, amount and transaction ID) is transmitted directly to Mollie and processed there. We do not store any complete credit card or

bank details ourselves, but merely receive information from Mollie regarding the status of the payment (successful/failed) as well as a transaction ID for order allocation.

Legal basis: Data processing is carried out on the basis of Article 6(1)(b) of the GDPR (performance of a contract) and our legitimate interest in secure and efficient payment processes in accordance with Article 6(1)(f) of the GDPR.

Data protection status Mollie acts as an independent data controller when processing the payment. Information regarding the processing of your data by Mollie can be found in their privacy policy.

Data processing within the EU: Mollie is based in the Netherlands and processes your payment data within the EU / European Economic Area. As a rule, no transfer to third countries takes place. Where a transfer to the relevant payment schemes is necessary for individual payment methods, this is carried out on the basis of appropriate safeguards pursuant to Article 46 of the GDPR.

Mollie's privacy policy: https://www.mollie.com/privacy.

9.2 PayPal

Provider: PayPal (Europe) S.à r.l. et Cie, S.C.A., 22-24 Boulevard Royal, L-2449 Luxembourg (hereinafter "PayPal"). PayPal acts as an independent controller. When selecting this payment method, the data required for payment processing (e.g. name, email address, purchase amount) is automatically transmitted to PayPal.

Legal basis: Art. 6(1)(b) GDPR.

Privacy Policy: https://www.paypal.com/de/webapps/mpp/ua/privacy-full.

9.3 Accounting: Lexware Office

To issue invoices, manage financial accounting and comply with our statutory retention obligations under tax and commercial law, we use the cloud-based software Lexware Office. The provider is Haufe-Lexware GmbH & Co. KG, Munzinger Straße 9, 79111 Freiburg, Germany. Billing data (name, address, email address, description of services, invoice amount) is transmitted to and processed by this provider.

Legal basis: Art. 6(1)© GDPR and Art. 6(1)(f) GDPR.

DPA: Concluded pursuant to Art. 28 GDPR. The DPA is available at: https://avv.lexware.de/lexware-office.

Note: We do not use any Google services (no Google Analytics, Google Fonts or Google Tag Manager). No data is transferred to Google.

10. Newsletter

Newsletter subscription follows a double opt-in (DOI) procedure:

- **Process:** After entering your email address, you will receive a confirmation email. Your subscription is only activated after you click the confirmation link.
- **Logging:** To provide legally compliant evidence of consent, we store your email address, the IP address at sign-up and confirmation, and the relevant timestamps.
- **Sending service:** Azure Communication Services (DPA concluded pursuant to Art. 28 GDPR).
- **Tracking:** We do not use newsletter tracking pixels (no open or click tracking).
- **Legal basis:** Art. 6(1)(a) GDPR and § 7(2)(3) UWG.
- **Retention period:** Your email address and consent record (DOI log) are stored for the duration of your consent. After unsubscription, the consent records are retained for evidentiary purposes for up to three years (Section 7(2) No. 2 UWG).

- **Unsubscribe:** You may withdraw your consent at any time with future effect - via the unsubscribe link in any newsletter or by email to privacy@sitzfritz.de.

11. Third-Country Transfers

We process personal data primarily within the EU/EEA. When using third-party services (Cloudflare, Microsoft), data may be transferred to third countries (in particular the USA). We use the following safeguards:

- EU-U.S. Data Privacy Framework (for certified US providers).
- Standard Contractual Clauses (SCCs) pursuant to Art. 46(2)© GDPR.
- Microsoft's specific EU Data Boundary commitment.

Information on the specific transfer mechanisms in use is available on request.

12. Cookies, Local Storage and Analytics Technologies

We use technically necessary cookies and local storage entries on our website, and — with your explicit consent — privacy-friendly, anonymised usage analytics on our own infrastructure (no third-party analytics provider).

Technically necessary entries (no consent required, § 25(2) TDDDG)

Name	Retention	Purpose
`sitzfritz_cookie_consent`	12 months	Stores your privacy consent decision
`session-token`	30 days	Login session (authentication)
`NEXT_LOCALE`	12 months	Language preference (DE/EN)
`Cloudflare Turnstile`	up to 30 min.	Bot protection on forms (Cloudflare, Inc., USA)

Analytics entries (consent required, Art. 6(1)(a) GDPR)

Name	Retention	Purpose
`sitzfritz_analytics_unique`	12 months	First-visit detection (local, no third party)
`sf_analytics_sid`	30 minutes	Anonymous session ID; groups related page views into one session (local, no third party)

Anonymised Usage Analytics (Opt-In)

With your consent, we collect anonymised usage statistics exclusively on our own infrastructure (Azure Table Storage, Germany). In addition to page views, we process anonymous interaction events (e.g. scroll depth, clicks on outbound links and downloads, and technical errors) in order to improve the website. No data is shared with third-party analytics services and no cross-device profiles are created.

The following data points are collected:

- Hashed IP address (SHA-256 + salt, truncated to 16 characters — not reversible)
- Browser type (user agent)
- URL path visited
- Referring website (referrer)

- Time spent on page
- Screen resolution
- Language setting
- First-visit flag (anonymised)
- Anonymous session ID (randomly generated, no personal reference)
- Approximate location (country) derived from the IP address
- Event type (page view, scroll depth, click, download, technical error, goal completion)
- Event detail (e.g. scroll depth in percent, outbound link target, file name, error message)
- Campaign parameters of the calling URL (utm_source, utm_medium, utm_campaign), where present

The IP address is processed solely to derive the approximate location (country) and to form the hash value, and is not stored in plain text.

Retention: 14 months from collection; automated deletion thereafter. **Withdrawal:** At any time via the 'Cookie Settings' link in the website footer, with effect for the future.

We do not use any Google services (no Google Analytics, Google Fonts or Google Tag Manager).

We honour automated privacy signals sent by your browser such as Do Not Track (DNT) and Global Privacy Control (GPC): our analytics only start after explicit consent in any case; where such a signal is set, analytical processing is additionally suppressed regardless of any consent.

As part of its bot detection process, Cloudflare Turnstile may set functional cookies or LocalStorage entries (technically necessary, § 25(2) TDDDG).

13. Retention Periods and Erasure

Personal data is erased once it is no longer required for the purpose for which it was collected.

Data category	Retention period
Account data	Duration of active use; erasure upon contract termination.
Invoices / accounting records	10 years (§ 257 HGB, § 147 AO).
Cloud sync data	Until consent is withdrawn or account deleted; max. 30 days after withdrawal.
Server log files	14 days (security purposes).
Anonymised visitor statistics	14 months (only with consent).
Newsletter sign-up records (DOI log)	Duration of consent; proof records up to 3 years after unsubscription.

14. Technical and Organisational Measures (TOM)

We implement appropriate technical and organisational measures pursuant to Art. 32 GDPR to protect personal data, including in particular:

- Encryption in transit (TLS/HTTPS) and at rest.
- Access controls and role-based permission management.
- Regular backups and disaster recovery procedures.

- Monitoring and security logging.
- Regular patch management processes.
- Planned penetration testing / security reviews.

Details of specific measures are available on request and to the extent permitted by data protection law (in particular in the context of a DPA).

15. Account, Sign-in and Authentication

For the registration, sign-in and management of your user account we operate a self-hosted authentication solution (identity and access management based on open-source software). It runs exclusively on our own infrastructure (auth.sitzfritz.de, Microsoft Azure, Region Germany West Central).

Self-hosting: We operate this solution entirely ourselves. No authentication or account data is transmitted to the company behind the software used; there is no data-processing relationship with that provider in this respect.

Data processed: Email address, name, pseudonymous user ID, roles and permissions, sign-in timestamps, and the session and token data and IP address technically required to perform the sign-in.

Legal basis: Art. 6(1)(b) GDPR (provision of the account / performance of contract) and Art. 6(1)(f) GDPR (IT security, abuse prevention).

Sign-in via Google or Microsoft (optional): Optionally, you may sign in via an external provider (Google or Microsoft). Only if you actively choose this does authentication take place with the respective provider; data is then exchanged with that provider under its own responsibility (see its privacy policy). Without your active choice, no transfer to these providers occurs.

Storage location: EU (Germany, Microsoft Azure Germany West Central).

Retention: For the duration of the existing user account; deletion after termination of the contractual relationship, unless statutory retention obligations apply.

16. Your Rights as a Data Subject

Under the GDPR you have the following rights:

- Right of access to data processed about you (Art. 15 GDPR).
- Right to rectification of inaccurate data (Art. 16 GDPR).
- Right to erasure ('right to be forgotten', Art. 17 GDPR).
- Right to restriction of processing (Art. 18 GDPR).
- Right to data portability (Art. 20 GDPR).
- Right to object to processing based on legitimate interests (Art. 21 GDPR).
- Right to withdraw consent with future effect (Art. 7(3) GDPR).
- Right to lodge a complaint with the competent supervisory authority (Art. 77 GDPR).

Competent supervisory authority:

State Commissioner for Data Protection and Freedom of Information of North Rhine-Westphalia (LDI NRW)
Kavalleriestr. 2-4, 40213 Düsseldorf, Germany
poststelle@ldi.nrw.de · www.ldi.nrw.de

To exercise your rights, please contact: privacy@sitzfritz.de.

Withdrawal of consent for website analytics: You may withdraw your consent to usage analytics at any time via the 'Cookie Settings' link in the website footer.

17. Changes to This Privacy Policy

Any changes to this Privacy Policy will be published here. In the event of material changes (e.g. new processing purposes, new service providers, new third-country transfers), registered users will additionally be notified by email. The date of the most recent update is always shown in the page header.