

DATENSCHUTZERKLÄRUNG — ERWEITERUNG MITGLIEDERBEREICH

Die EnergieOase Membership

Stand: 25. August 2026

Deine Daten bleiben in Deutschland.

Der gesamte Mitgliederbereich läuft auf Servern in deutschen Rechenzentren (Falkenstein und Nürnberg).

Deine Gesundheitsdaten werden verschlüsselt gespeichert und verlassen Deutschland nicht.

Diese Erweiterung ergänzt die bestehende Datenschutzerklärung der EnergieOase (die-energie-oase.de/datenschutzerklaerung).

A. Geltungsbereich dieser Erweiterung

Diese Erweiterung gilt für den Mitgliederbereich mitglieder.die-energie-oase.de und beschreibt alle Verarbeitungen, die über die allgemeine Website-Datenschutzerklärung hinausgehen. Die allgemeinen Abschnitte (Verantwortlicher, Logdateien, Verschlüsselung, Cookies, Betroffenenrechte) gelten unverändert.

B. Verantwortliche Stelle

Die EnergieOase Alte Eitzer Str. 12 · 27283 Verden (Aller) · Deutschland E-Mail: info@die-energie-oase.de · Tel: +49 172 6155068

Für Anfragen zum Mitgliederbereich zusätzlich: mitglieder@die-energie-oase.de

C. Verarbeitung im Rahmen der Mitgliedschaft

1. Registrierung und Mitgliederkonto

Verarbeitete Daten: Vor- und Nachname, E-Mail-Adresse, Postanschrift, Geburtsdatum, Telefonnummer, gewählter Tarif (Solo/Paar), Passwort (gehasht), Tarifname, Einwilligungsprotokoll (Zeitstempel + IP), bei Paar-/Family-Tarif Daten der mitversicherten Personen.

Zweck: Vertragsabschluss und -durchführung, Identifizierung, Kommunikation. Vor dem Vertragsschluss wird die angegebene E-Mail-Adresse durch einen Bestätigungs-Link überprüft (Double-Opt-In); wird er nicht binnen sieben Tagen aufgerufen, werden die Anmeldedaten gelöscht.

Rechtsgrundlage: Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung) sowie Art. 6 Abs. 1 lit. c DSGVO (rechtliche Verpflichtungen).

Speicherdauer: Während der Mitgliedschaft sowie gesetzliche Aufbewahrungsfristen (z. B. § 257 HGB, § 147 AO — 10 Jahre für rechnungsrelevante Daten).

2. Zahlungsabwicklung

Die Beitragszahlung erfolgt per **Überweisung** auf das Konto der EnergieOase. Es ist **kein Zahlungsdienstleister zwischengeschaltet**.

Verarbeitete Daten: Name, Verwendungszweck, Betrag und Buchungsdatum aus dem Kontoauszug sowie die Rechnungsdaten.

Zweck: Zuordnung der Zahlung zum Mitgliedskonto und Rechnungsstellung.

Rechtsgrundlage: Art. 6 Abs. 1 lit. b DSGVO.

Drittland: keiner — die Daten verbleiben bei der EnergieOase und ihrer Bank.

3. Hosting des Mitgliederbereichs (Hetzner)

Auftragsverarbeiter: Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Deutschland.

Verarbeitete Daten: Sämtliche im Mitgliederbereich gespeicherten Daten (Konto, Inhalte, Gesundheitsdaten).

Zweck: Bereitstellung der Plattform-Infrastruktur.

Standort: Rechenzentren in Deutschland (Falkenstein/Nürnberg).

Sicherheitsmaßnahmen:

- Vollverschlüsselte Festplatten (LUKS)
- TLS 1.3 für alle Verbindungen
- Regelmäßige, verschlüsselte Sicherungen
- Härtung des Servers (fail2ban, UFW, automatische Sicherheitsupdates)
- Audit-Log für alle Zugriffe auf sensible Daten

Rechtsgrundlage: Art. 6 Abs. 1 lit. b und f DSGVO. AVV gemäß Art. 28 DSGVO besteht.

4. Newsletter und Marketing (Mailchimp)

Auftragsverarbeiter: Intuit Mailchimp, 405 N Angier Ave NE, Atlanta, GA 30308, USA.

Verarbeitete Daten: E-Mail-Adresse, Name, Mitgliedsstatus, Öffnungs- und Klick-Statistiken.

Zweck: Versand von Newslettern, Mitglieder-Informationen, Veranstaltungshinweisen.

Rechtsgrundlage: Art. 6 Abs. 1 lit. a DSGVO (Einwilligung, Double-Opt-In).

Drittlandtransfer: USA. Die Übermittlung erfolgt auf Grundlage des **EU-US Data Privacy Framework** (Angemessenheitsbeschluss vom 10.07.2023) sowie ergänzender Standardvertragsklauseln.

Hinweis: Die Einwilligung kann jederzeit über den Abmelde-Link in jeder Mail widerrufen werden.

5. Push-Benachrichtigungen (App)

Verarbeitete Daten: Adresse des Push-Endpunkts deines Browsers, die zugehörigen öffentlichen Schlüssel und ein Zeitstempel. Darüber hinaus keine Gerätekennung.

Zweck: Erinnerungen an gebuchte Termine und Hinweise auf neue Inhalte im Mitgliederbereich.

Rechtsgrundlage: Art. 6 Abs. 1 lit. a DSGVO (Einwilligung). Die Benachrichtigungen sind freiwillig — ohne Einwilligung funktioniert die App vollständig.

Empfänger: Die Zustellung läuft technisch über den Push-Dienst deines Browserherstellers (Google bei Chrome, Mozilla bei Firefox, Apple bei Safari). Diese Dienste erhalten die Endpunkt-Adresse und die verschlüsselte Nachricht; je nach Hersteller findet die Verarbeitung auch in den USA statt.

Speicherdauer: Bis zum Widerruf oder bis der Endpunkt ungültig wird (z. B. nach Deinstallation der App).

Widerruf: Jederzeit in den Benachrichtigungs-Einstellungen im Profil oder in den Einstellungen deines Browsers. Der gespeicherte Endpunkt wird dann gelöscht.

D. Gesundheitsdaten (Art. 9 DSGVO) — besondere Kategorien personenbezogener Daten

Wichtiger Hinweis: Gesundheitsbezogene Daten genießen besonderen Schutz nach Art. 9 DSGVO. Die Verarbeitung erfolgt ausschließlich auf Grundlage Ihrer **ausdrücklichen, gesonderten Einwilligung** (Art. 9 Abs. 2 lit. a DSGVO).

1. HRV-Messungen (Herzfrequenzvariabilität, Nilas MV)

Verarbeitete Daten: Messberichte (PDF, ggf. Rohdaten), Datum, Messparameter, vom Mitglied oder Coach hinzugefügte Notizen.

Zweck: Persönlicher Verlauf, Auswertung, Coaching-Grundlage.

Speicherort: Verschlüsselt auf Hetzner-Server in Deutschland. Pro Mitglied separater Schlüssel; Zugriff ausschließlich durch das Mitglied und — nach individueller Freigabe — durch Aarti oder eine:n autorisierte:n Coach.

2. Bio-Well-Messungen (Bio-Well GDV)

Verarbeitete Daten: Bilder, Berichte, Auswertungen, Energiefelder-Visualisierungen, vom Mitglied oder Coach hinzugefügte Notizen.

Zweck: wie HRV.

Speicherort und Zugriff: wie HRV.

3. Atem- und Soundmodule

Verarbeitete Daten: Individuell für das Mitglied erstellte Audiodateien (MP3 oder Streaming-Format), zugeordneter Zeitstempel.

Zweck: Bereitstellung persönlicher Audio-Anwendungen.

Speicherort und Zugriff: wie HRV; pro Datei konfigurierbar (Streaming-only oder Download erlaubt).

4. Einwilligung, Freigabe, Löschung

- **Einwilligung:** Vor der ersten Verarbeitung erfolgt eine separate, granulare Einwilligung (Upload, Speicherung, Verlauf, optionale Freigabe an Coach).
- **Freigabe:** Standardmäßig sehen nur Sie Ihre Gesundheitsdaten. Eine Freigabe an Aarti oder eine:n Coach kann **pro Datei** im Account aktiviert oder widerrufen werden.
- **Löschung:** Sie können einzelne Dateien oder den gesamten Bereich jederzeit löschen. Bei Beendigung der Mitgliedschaft werden Gesundheitsdaten standardmäßig nach **30 Tagen automatisch gelöscht**, sofern Sie keine längere Aufbewahrung wünschen.
- **Export:** Sie können Ihre Daten jederzeit als ZIP-Datei aus dem Account exportieren.

5. Empfänger und Weitergabe

Gesundheitsdaten werden **nicht** an Dritte weitergegeben — auch nicht zu Marketing-, Statistik- oder Forschungszwecken. Ausnahme: gesetzliche Verpflichtung (z. B. richterliche Anordnung).

E. Community-Funktionen

1. Profile

Verarbeitete Daten: Profilbild (freiwillig), Anzeigenname, Selbstbeschreibung, sichtbare Interessen.

Sichtbarkeit: Vom Mitglied pro Feld einstellbar — öffentlich nicht möglich, sondern nur „alle Mitglieder“ oder „nur ich“.

Rechtsgrundlage: Art. 6 Abs. 1 lit. a DSGVO (Einwilligung).

2. Direktnachrichten, Forum und Chat

Verarbeitete Daten: Nachrichten- und Beitragsinhalte, Zeitstempel, Empfänger:in.

Zweck: Kommunikation zwischen Mitgliedern.

Speicherdauer: Während der Mitgliedschaft. Nach Beendigung anonymisiert oder gelöscht innerhalb von 90 Tagen.

Moderation: Ausschließlich Aarti kann bei Verdacht auf einen Verstoß Nachrichten einsehen und löschen. Inhalte werden nicht systematisch ausgewertet.

F. Buchungssystem (Amelia)

Verarbeitete Daten: Mitgliedsstatus, gebuchte Leistung, Termin, Bezahlmethode, Stornierungen, Wartelisten-Position.

Zweck: Terminbuchung und Verwaltung.

Rechtsgrundlage: Art. 6 Abs. 1 lit. b DSGVO.

Speicherdauer: 3 Jahre nach letzter Buchung (Beweissicherung gemäß § 199 BGB), darüber hinaus rechnungsbezogene Daten 10 Jahre (§ 147 AO).

G. Cookies und Tracking im Mitgliederbereich

Im Mitgliederbereich werden ausschließlich **technisch notwendige Cookies** (Session, CSRF-Token, Authentifizierung) gesetzt. **Kein Tracking, kein Marketing-Cookie ohne separate Einwilligung.**

H. Ihre Rechte (Art. 12–22 DSGVO)

Es gelten dieselben Rechte wie in der allgemeinen Datenschutzerklärung:

- **Auskunft** (Art. 15)
- **Berichtigung** (Art. 16)
- **Löschung** (Art. 17) — beachten Sie gesetzliche Aufbewahrungsfristen
- **Einschränkung** (Art. 18)
- **Datenübertragbarkeit** (Art. 20) — ZIP-Export im Account
- **Widerspruch** (Art. 21)
- **Widerruf der Einwilligung** (Art. 7 Abs. 3) — jederzeit, mit Wirkung für die Zukunft
- **Beschwerde bei der Aufsichtsbehörde** (Art. 77) — zuständig: Landesbeauftragte für Datenschutz Niedersachsen, Prinzenstr. 5, 30159 Hannover, <https://fd.niedersachsen.de>

Self-Service im Account

- **Auskunft / Export:** „Mein Konto – Datenexport“ – ZIP-Download
- **Löschung:** „Mein Konto – Konto löschen“ – Bestätigung per Mail
- **Einwilligungen verwalten:** „Mein Konto – Einwilligungen“

I. Datensicherheit

Maßnahme	Umsetzung
Verschlüsselung Verbindung	TLS 1.3
Verschlüsselung Server	LUKS Full-Disk-Encryption
Verschlüsselung sensible Dateien	libsodium (XSalsa20-Poly1305), pro Mitglied separater Schlüssel
Zugriff	Rollenbasiert; Verwaltungszugänge zusätzlich geschützt
Audit-Log	Jeder Zugriff auf Gesundheitsdaten wird protokolliert
Passwort-Speicherung	Nach dem aktuellen Stand der Technik gehasht, niemals im Klartext
Brute-Force-Schutz	fail2ban + Rate-Limiting
Update-Zyklus	Wöchentliche Sicherheitsupdates + Plugin-Monitoring

J. Änderungen dieser Erklärung

Wesentliche Änderungen werden den Mitgliedern mindestens **6 Wochen vor Wirksamwerden** in Textform mitgeteilt.

Fassung 2.0 · Stand der Erweiterung: 2026-08-25 Verweis auf Haupt-Datenschutzerklärung:
die-energie-oase.de/datenschutzerklaerung