Datenschutz & IT-Sicherheit

Wie wir personenbezogene Daten schützen – verständlich erklärt, ohne Marketing-Floskeln.

Kurzfassung: Wir speichern und verarbeiten Nutzerdaten DSGVO-konform, bevorzugt auf Servern innerhalb der EU, und setzen zeitgemäße Verschlüsselung sowie Zugriffsschutz ein. Verbindliche Details stehen in unserer Datenschutzerklärung und den jeweils gültigen Vertrags-/Projektunterlagen.

Worum es hier geht

Dieses Factsheet beschreibt unsere Datenschutz- und Sicherheitsprinzipien auf hoher Ebene. Es ersetzt keine Rechtsberatung und ist keine vollständige Datenschutzerklärung, sondern ein transparenter Überblick für die Öffentlichkeit.

Unsere Sicherheits- und Datenschutz-Standards

DSGVO (EU 2016/679)	Verarbeitung nach DSGVO-Grundsätzen: Zweckbindung, Datenminimierung, Transparenz sowie Integrität und Vertraulichkeit.
Speicherort / Hosting	Hosting und Speicherung bevorzugt innerhalb der EU (soweit technisch und vertraglich möglich).
Verschlüsselung (Transport)	Datenübertragung über TLS/HTTPS.
Verschlüsselung (Speicher)	Verschlüsselung ruhender Daten (z. B. AES-256 oder gleichwertig, abhängig von der eingesetzten Systemkomponente).
Zugriffsschutz	Prinzip der minimalen Rechte (Least Privilege), rollenbasierte Zugriffe, Multi-Faktor-Authentifizierung wo verfügbar.
Protokollierung	Relevante System- und Sicherheitsereignisse werden protokolliert, um Vorfälle untersuchen zu können.
Backups & Wiederherstellung	Regelmäßige Backups und geprüfte Wiederherstellungsprozesse, um Datenverluste zu minimieren.
Auftragsverarbeitung	Einsatz von Dienstleistern nur auf Basis geeigneter Verträge (insb. AVV) und dokumentierter Sicherheitsmaßnahmen.
Löschkonzept	Daten werden nur so lange gespeichert, wie es für Zwecke und gesetzliche Pflichten erforderlich ist.
Incident Response	Definierte Prozesse für Sicherheitsvorfälle (Erkennung, Eindämmung, Behebung, Kommunikation).

Wichtige Abgrenzung (ehrlich)

Kein System ist „100 % sicher“. Unser Anspruch ist es, Risiken durch Technik, Prozesse und Kontrollen konsequent zu reduzieren und transparent zu kommunizieren, wie Daten geschützt werden.

Deine Rechte nach DSGVO (Kurzüberblick)

Du hast unter anderem folgende Rechte (je nach Verarbeitung und Rechtsgrundlage):

- Auskunft über die Verarbeitung deiner Daten
- Berichtigung unrichtiger Daten
- Löschung („Recht auf Vergessenwerden“), soweit keine Aufbewahrungspflichten entgegenstehen
- Einschränkung der Verarbeitung
- Widerspruch gegen bestimmte Verarbeitungen
- Datenübertragbarkeit (soweit anwendbar)
- Beschwerderecht bei einer Datenschutz-Aufsichtsbehörde

Praktische Schutzmaßnahmen (Auszug)

- **Security by Design:** Sicherheitsanforderungen fließen früh in Architektur und Entwicklung ein.
- **Härtung & Updates:** Regelmäßige Updates, Patch-Management und Minimierung unnötiger Dienste.
- **Passwort-/Account-Schutz:** MFA wo möglich, sichere Reset-Prozesse, Schutz vor Brute-Force.
- **Trennung von Umgebungen:** Entwicklungs-/Test-/Produktivsysteme getrennt, Zugriff eingeschränkt.
- **Monitoring:** Alarmierung bei auffälligen Ereignissen (z. B. Login-Anomalien, Fehlerraten).
- **Backups:** Wiederherstellung regelmäßig geprüft (nicht nur „Backup vorhanden“).
- **Datensparsamkeit:** Erhebung nur, wenn notwendig; klare Zweckdefinition.
- **Vendor Management:** Bewertung kritischer Dienstleister, Vertrags- und Sicherheitsanforderungen.

Transparenz & weitere Details

Die verbindlichen Details findest du in unserer Datenschutzerklärung, ggf. Cookie-Hinweisen sowie in den jeweils gültigen Vertrags- und Projektunterlagen. Dort benennen wir u. a. Zwecke, Rechtsgrundlagen, Empfänger/Auftragsverarbeiter, Speicherdauern und Kontaktwege.

Offizieller Gesetzestext (DSGVO): https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=de

Kommunikation & Kontakt

Kontaktwege und die zuständige Stelle für Datenschutzanfragen sind in der Datenschutzerklärung/Impressum aufgeführt. Bitte sende keine sensiblen Dokumente über unsichere Kanäle, sofern nicht ausdrücklich vorgesehen.

Hinweis: Dieses Dokument ist ein öffentlicher Überblick und kann sich mit der Weiterentwicklung von Systemen, Dienstleistern oder rechtlichen Anforderungen ändern. Maßgeblich sind stets die aktuellen veröffentlichten Policies und Vertragsunterlagen.