



CyberWehr
RISK MANAGEMENT SOLUTIONS GMBH

Wir sind Ihre Ansprechpartner in allen betrieblichen Datenschutzfragen
DSG / DSGVO

Sind Ihre Daten wirklich sicher - auch in der Cloud?

Strategische Datenschutzkonzepte, die

- rechtlich greifen, technisch umsetzbar und im Alltag tragfähig sind
- ganzheitliche Risikoanalysen inkl. Cybersecurity
- Datenschutz vor Missbrauch, Diebstahl, Offenlegung gegenüber Unbefugten
- ohne Bürokratiemonster
- Durchführung von Datenschutz-Audits

TÜV
Technischer
Dienstleistung

Datenschutz-Compliance ist Führungsverantwortung. Nicht nur ein IT-Thema.

Wer ihn ignoriert, bezahlt mit Geld, Reputationsschäden und der persönlichen Haftung. **Es ist Ihre gesetzliche Verpflichtung + Verantwortung**, dass die Datenbearbeitung **rechtmässig** erfolgt. Geht etwas schief, sind Sie in der Haftung. Denn Sie sind gem. der DSGVO/DSG-VO verpflichtet, den **Datenschutz durch technische und organisatorische Massnahmen** so zu gestalten, dass die Datenschutzvorschriften sichergestellt und eingehalten sind und Sie diese auch nachweisen können. Die Bearbeitung der Personendaten muss auf das für den Verwendungszweck nötige Mindestmass (Speicherbegrenzung) beschränkt sein. Datenschutz ist längst kein juristischer Nebenschauplatz mehr. Er ist **zentrale Voraussetzung für Vertrauen**, Geschäftstätigkeit in der EU – Ihre Lizenz für den digitalen Markt.

Egal, ob Ihr Unternehmen in der Schweiz, in der EU oder grenzüberschreitend arbeitet:

Datenschutzgesetze gelten – und sie greifen hart durch. Auch beim Einsatz der Cloud oder von KI.

Was ist zu beachten?

Die **EU-DSG-VO** schützt personenbezogene Daten in der gesamten EU – und das auch dann, wenn die Datenverarbeitung **ausserhalb** der EU erfolgt (z. B. durch Schweizer Unternehmen mit EU-Kunden). Die Schweiz hat mit dem revidierten DSG ein vergleichbares Datenschutzniveau der EU eingeführt und profitiert vom freien Datenverkehr ohne erforderliche separate Datenschutznachweise.

⇒ Aber Sie müssen die gesetzlichen Datenschutzregeln kennen – und anwenden.

Was bedeutet das konkret für Sie?

- **Rechtssicherer Umgang mit personenbezogenen Daten:**
Verarbeitung nur mit Einwilligung oder klarer gesetzlicher Grundlage.
- **Informationspflichten einhalten (Datenschutzerklärung, Auskunftsrechte):**
Korrekte Datenschutzerklärung, Cookie/Plugins-Management, klare Auskunftsprozesse.
- **Technische und organisatorische Schutzmassnahmen auf Vollständigkeit überprüfen:**
„Privacy by Design & Default“ – Datenschutz von Anfang an mitdenken.
- **Pflicht zur Transparenz & Rechenschaft („Accountability“):**
Sie müssen jederzeit **nachweisen können**, wie, warum und wo Daten verarbeitet werden.
- **Rechte der Betroffenen einhalten:**
Auskunft, Widerspruch, Löschung, Datenübertragbarkeit – **auch in 30 Tagen**.

- **Cloud-Nutzung & internationale Datenübertragung prüfen:**
Besonders kritisch bei Dienstleistern ausserhalb der EU – Handlungsbedarf!
 - **Pflicht zur Meldung von Datenschutzverletzungen:**
Fehlende Prozesse führen schnell zu Bussgeldern und Reputationsverlust.
 - **Datenschutz-Folgenabschätzung bei sensiblen Daten:**
Gerade im Gesundheitsbereich zwingend erforderlich.
-

Ein Klarer Fahrplan statt ein Paragraphen-Dschungel.

Wir liefern Ihnen **konkrete Handlungsempfehlungen, praxisnahe Werkzeuge** und auf Wunsch eine **automatisierte Softwarelösung**, die Ihre Datenschutzpflichten nachweisbar und effizient abbildet.

Ob KMU, Industrie, Altersheim oder Klinik – Sie bekommen eine branchentypische Lösung, die funktioniert und geprüft standhält.

Denn Datenschutz-Compliance schafft nicht nur Rechtssicherheit, sondern stärkt das Vertrauen Ihrer Kunden, schützt Ihre Reputation und sichert Ihre digitale Zukunft.

Führen Sie einen Sicherheits-Check durch; prüfen und kontrollieren Sie Ihre technischen und organisatorischen risikomindernden Massnahmen und Kontrollen.

Ermitteln Sie mit unserer Unterstützung Ihre Risikoanalyse durch zur Identifikation der **Gefährdungen + Bedrohungen** für personenbezogene Daten, um dann in der Lage zu sein, mit geeigneten und angemessenen Schutzmassnahmen:

- Die unrechtmässige Datenverarbeitung
- Den unzulässigen Datenzugriff / Zugang
- Datenleaks, Spionage, Sabotage (abhören verändern blockieren)
- Unsicherheiten in der Datenübertragung
- Den Verlust, die Zerstörung oder Schädigung der Daten zu vermeiden und
- Die Verfügbarkeit der Daten auch während des Transports zu gewährleisten.

Kontaktieren Sie uns für Ihre individuelle Roadmap: **rechtskonform, dokumentiert und zukunftssicher.**

Schützen Sie heute, müssen Sie morgen nicht retten.