



CyberWehr

RISK MANAGEMENT SOLUTIONS GMBH

Monika Wehr ▪ +41 79 348 55 63 ▪ [info@cyberwehr-rms.ch](mailto:info@cyberwehr-rms.ch) ▪ 8803 Rüschlikon, Alte Landstrasse 109

---

## Datenschutzberatung hat das Ziel der Datenschutz-Rechtskonformität

### Welche Gesetze kommen zur Anwendung?

Im Zentrum der Datenschutz-Grundverordnung (**DSGVO**) steht der Schutz für die Bürgerinnen und Bürger: sie sollen grundsätzlich die Hoheit über ihre eigenen Daten behalten. Die DSGVO schützt den einheitlichen und starken Datenschutz in der **EU**; bestehende nationale Gesetze in den einzelnen EU-Ländern wurden an die DSGVO angepasst und garantieren ein einheitliches Datenschutzniveau. Die Schweiz und UK als sogenannte Drittländer haben ebenso ihre Datenschutzgesetze (**DSG, Schweiz**) angepasst, auch um die Handelsbeziehungen mit der EU zu erleichtern. Das DSG tritt Mitte 2022 in Kraft ohne Übergangsfristen. Die DSGVO gilt **unabhängig davon, ob die Verarbeitung in der EU stattfindet oder nicht**. Sie gilt auch für alle Verarbeitungsvorgänge von personenbezogenen Daten, die von Verantwortlichen und Auftragsverarbeitern **mit Sitz in der EU** durchgeführt werden.

### Was regeln DSGVO und DSG? Gesetzliche Vorgaben, die in der Umsetzung im Unternehmen in den Geschäftsprozessen zu berücksichtigen sind:

Die DSGVO stellt die Verarbeitung personenbezogener Daten unter ein Verbot mit „Erlaubnisvorbehalt“. Damit die **Verarbeitung rechtmässig** ist, darf sie in der EU nur dann erfolgen, wenn eine **Einwilligung** der betroffenen Person oder eine rechtliche Verpflichtung vorliegt. Dieses Gebot wurde zwar in der Schweiz nicht 1:1 umgesetzt, so dass Unternehmen, sofern sie ihre Waren und Dienstleistungen in der EU anbieten, auch auf ihrer Webseite die Einwilligung des Lesers beim Speichern oder **Tracking** mit **Cookies** personenbezogener Daten mitberücksichtigen müssen. Die Rechtskonformität der **Webseite** ist demzufolge auch zu prüfen. In der **Datenschutzerklärung** muss der Verantwortliche seiner Informationspflicht nachkommen und erklären, wie die Daten von einer Organisation verarbeitet, d.h., wie diese Daten gesammelt, genutzt und ob sie an Dritte weitergegeben werden.

Strengere **Informations- und Auskunftspflichten** bei der Beschaffung von Personendaten und eine **Meldepflicht** beim Verlust von Personendaten (Datenschutzverletzung/Datenpanne) sollen zu mehr Transparenz führen. Die Verletzung dieser Pflichten wird mit schmerzhaften Geldbussen bestraft.

Datenschutz wird an die neuen technologischen Entwicklungen angepasst: verschiedene Vorschriften zu **Profiling** und automatisierten Einzelentscheidungen sowie zum Datenschutz durch Technik sollen den Schutz der persönlichen Daten weiter erhöhen.

Bürger:innen (Betroffene) können ihre Rechte, das **Recht auf Auskunft, Information, Widerspruch, Löschung der Daten und Datenübertragbarkeit** einfordern. Gewährleistungsziele wie Integrität, Vertraulichkeit und die Verfügbarkeit der Daten führen zu besonderen Anforderungen im Datenschutz. Datenschutz durch Technikgestaltung (**Privacy by Default**) und Datenschutzvorgaben in der Konstruktion und Gestaltung (**Privacy by Design**) von Geräten, Maschinen, Applikationen und Software erfordern einen risikobasierten Ansatz, eine Pflichtübung, nicht nur zur Risikoidentifikation, sondern auch zur Bestimmung **angemessener technischer und organisatorischer Schutzmassnahmen zur Erfüllung der** Gewährleistungsziele. Im Fall der Verarbeitung besonders sensibler Daten, z.B. Gesundheitsdaten, ist eine **Datenschutzfolgeabschätzung** eine zwingende Vorschrift. Ein besonderes Risiko stellen **Datenübertragungen ins nichteuropäische Ausland**, insbesondere auch i.F. der Ansässigkeit von Dienstleistern einer Cloud dar. Die gesetzliche Pflicht, «Accountability», zur Führung eines dokumentierten Verzeichnisses von Verarbeitungstätigkeiten, dient zum Nachweis gegenüber den Aufsichtsbehörden.

Wir stellen Ihnen einen Fahrplan zur pragmatischen Umsetzung der gesetzlichen Vorgaben für Ihr Unternehmen zur Verfügung.