CyberWehr
RISK MANAGEMENT SOLUTIONS GMBH
Monika Wehr ▪ +41 79 348 55 63 ▪ 8803 Rüschlikon, Alte Landstrasse 109

Roadmap - Datenschutz in der Praxis umsetzen:

Das DSG und die darin verankerte EU-DSGVO verpflichtet Unternehmen, die datenschutzrechtlichen Anforderungen punktuell und strukturell zu erfüllen. Das heisst insbesondere für die exportorientierten KMU: ein Unternehmen muss im Fall einer Datenschutzverletzung der Prüfung durch die Aufsichtsbehörde nicht nur standhalten, sondern auch nachweisen können, dass es zu einem bestimmten Zeitpunkt datenschutzkonform gearbeitet hat. Es muss der **dokumentierte** Nachweis (**"Accountability"**) geführt werden, dass man die datenschutzrechtlichen Anforderungen laufend, **auch für einen in der Vergangenheit liegenden Fall**, in der Unternehmenspraxis erfüllt.

Daher ist meine Empfehlung, dass Unternehmen (je nach Grösse) eine Datenschutzrichtlinie und/oder ein Datenschutzhandbuch erstellen sollten, um die datenschutzrechtlichen Anforderungen in ihrem Unternehmen zu adressieren.

Der Schutz der digitalen Zukunft eines Unternehmens beginnt damit, den gegenwärtigen Bestand personenbezogener Daten zu kennen, zu wissen, wo diese gespeichert sind und welche Massnahmen erforderlich sind, um unberechtigte Zugriffe oder sogar Datendiebstahl zu verhindern.

Erforderliche Schritte zur Umsetzung der Anforderungen gemäss DSG/DSGVO:

⇨ Optional: **Risikoanalyse ISO 27001/2** und Ermittlung des Gefahrenpotentials. Die beste Methode zur gezielten Bestimmung der Prioritäten risikomindernder Massnahmen.

⇨ **Informationssicherheits- und Datenschutz-Management**. Interne Datenschutz-Richtlinie. Notfallplanung zur vorbereiteten Reaktion auf eine Datenpanne.

⇨ Umfassende Orientierung über **gesetzlichen Anforderungen**, um **Geldbussen** gem. Art. 83 DSGVO durch unzureichende Einhaltung von Informations-, Speicher- oder Löschpflichten zu vermeiden.

⇨ **Die Rechte der Betroffenen:** Auskunft, Information, Vergessen-werden, Datenportabilität etc. gem**.** Art. 25, 28, 29 revDSG/Art. 12 – 14, 15 – 19 – 21, 30 DSGVO. Einführung eines Beschwerdemanagementsystem mit Fristen-Verwaltung (Löschkonzept). Sind die Geschäftsprozesse und Systeme geeignet, um bspw. der Informationspflicht und der Löschung personenbezogener Daten sofort nachzukommen?

⇨ **Verzeichnis der Be-(Ver)arbeitungstätigkeiten (VVT),** Art. 5 Bst. f+g revDSG/Art. 30 DSGVO: Dokumentation & Nachweis der einzelnen Prozesse, Verfahrensbeschreibung für jede einzelne Verarbeitungstätigkeit mit Angaben zur Rechtmässigkeit, Verarbeitungszweck, Richtigkeit und Aktualität der Daten. Nachweis der geeigneten technischen und organisatorischen Massnahmen.

⇨ **Datenschutz durch Technikgestaltung Datenschutz „by design“ und „by default“** Art. 7 revDSG Abs. 1+2/Art 25 Abs. 2 + 32 DSGVO: geeignete technische und organisatorische Massnahmen ergreifen, um die Verarbeitung personenbezogener Daten systematisch zu schützen: Schutz der Daten vor Verletzungen der Integrität, Vertraulichkeit und Verfügbarkeit etc.

⇨ **Auftrags(be)verarbeitung,** Art. 9 Abs. 3 revDSG/Art. 28 DSGVO. Wann ist ein Vertrag bei der Einbindung externer Dritter, z.B. Steuerberater, Lohnbuchhaltung in der Datenverarbeitung zu unterzeichnen?

⇨ **EuGH Urteil Schrems II vom 12.7.2020** – rechtliche Rahmenbedingungen der Cloud - entsprechen sie dem Datenschutz-Sicherheitsstandard? Ist ein limitierter Zugang oder ein „public access“ sinnvoll? Achtung: ist der Cloud Anbieter in den USA oder einem Drittland angesiedelt ist, besteht ggfs. akuter Handlungsbedarf.

⇨ Sind Ihre **Mitarbeiter geschult gem. Art 39 DSGVO** für den Fall einer Datenschutzverletzung, auf die Beschwerde eines Betroffenen oder auf ein Mail mit einer Schadsoftware angemessen reagieren zu können?

⇨ Meldungen einer **Datenschutzverletzung** (Datenpanne) gem. revDSG Art. 24 neu/DSGVO Art. 32-34 an Aufsichtsbehörde/MELANI. Besteht ein **Notfallkonzept** im Krisenfall?

⇨ **„Accountability“** gem. Art 30 DSGVO: Sie sind verpflichtet, die Grundwerte des Datenschutzes: Transparenz, Datenminimierung, Vertraulichkeit, Integrität und Verfügbarkeit einzuhalten. Gegenüber den Aufsichtsbehörden besteht eine gesetzliche Nachweispflicht.

⇨ Aktualisierung der Webseiten-**Datenschutzerklärung**

⇨ **Automatisierte Softwarelösung:** Mittels einer Softwarelösung kann jedes Unternehmen den Datenschutz ohne eigenes Know-How und ohne viel Aufwand umsetzen, sofern der Datenschutzkoordinator gute EDV-Kenntnisse hat. Die Erstellung jedweder Datenschutz-Dokumentation kann voll automatisiert mit unserer Software, eine webbasierte Lösung, durchgeführt werden.