

Wer nicht den gesetzlich vorgeschriebenen Datenschutz und entsprechende Maßnahmen nicht lückenlos nachweisen kann, kann laut DSGVO (oder auch GDPR - General Data Protection Regulation) mit Bußgeldern bis zu 20 Millionen Euro beziehungsweise vier Prozent des - weltweiten - Konzernumsatzes bestraft werden. Denn nach dem Markttortprinzip greift die Datenschutz-Grundverordnung für jede Geschäftsform, sprich für alle, die Waren und Dienstleistungen in der EU anbieten oder das Verhalten von Personen digital beobachten.

Ziel der Gesetzgeber ist es, das persönliche Recht auf datenschutzfreundliche Voreinstellungen (Stichworte: Privacy by Default und Privacy by Design) und das "Vergessenwerden" durchzusetzen, die Datennutzung transparent zu machen und Datentransfers zu vereinfachen.

Erste Schritte auf dem Weg zu DSGVO-Konformität

- DSGVO-kompetente Datenschutzbeauftragte einsetzen
- Stammdatenverwaltung auf den neuesten Stand bringen
- Unstrukturierte Daten erfassen und analysieren (E-Mail, Dokumente, etc.)
- Data Mapping zur Identifikation von Datensätzen, ihrer Herkunft und Sensibilität
- Daten in Sicherheitsstufen klassifizieren und dies dokumentieren
- Alle Anwendungen und Ablagen systematisch abarbeiten
- Dokumentation der Verarbeitungsvorgänge anlegen
- Datenschutz-Folgeabschätzung für die einzelnen Vorgänge nicht vergessen
- Einwilligungserklärungen, AGBs, SLAs, etc. überprüfen
- Software installieren, die Angriffe und Datendiebstahl erkennt (z.B. Intrusion Detection, Threat Intelligence ...) und das Notfallmanagement anschiebt
- Notfallmanagement/Desaster Recovery einführen, 72-Stunden-Meldefrist berücksichtigen
- Unerlaubten Datenfluss unterbinden
- Zweckgebundenheit der erhobenen Daten sicherstellen
- Informationsverpflichtung gegenüber den Datengebern nicht vergessen