EU Datenschutz-Grundverordnung & IT-Sicherheit

Ing. Mag. Dr. Vincenz Leichtfried
VL@LV7.ms, + 43 650 43 650 85

Hardfacts

- EU Datenschutz-Grundverordnung für die Verarbeitung von personenbezogenen Daten muss bis 25. Mai 2018 umgesetzt werden
- Trifft Personen, Unternehmen, Behörden, Vereine, etc..
- Ausnahmen für private und familiäre Tätigkeiten. Abhängig vom Umfang fallen online Aktivitäten (z.B. Blogs, Social Media Postings…) nicht in diese Ausnahme
- Gilt auch für analoge Verarbeitung auf Papier, wenn es sich um eine strukturierte Ablage handelt
- Datenschutz hat juristische, technische und organisatorische Auswirkungen
- Cyberkriminalität ist in den letzten Jahren stark gestiegen
- Über 70 % aller Datenschutzvorfälle entstehen durch menschliches Versagen
- Kryptotrojaner in Ransomsoftware verzeichnen das stärkste Wachstum

Beteiligte

Ansprechpartner für den Betroffenen ist immer nur der Verantwortliche bzw. gegebenenfalls sein Datenschutzbeauftragter.

Geldstrafen

Bei Nichteinhaltung der Datenschutz-Grundverordnung sind Strafen bis zu 20 Mio. Euro oder 4 % des weltweiten Konzernumsatzes vorgesehen (je nachdem was höher wiegt). Ein wesentlicher Faktor für das Strafmaß ist die Konformität der Umsetzung mit der Datenschutz-Grundverordnung und wie diese dokumentiert wurde. **Auslöser können unter anderem sein**:

- Umsetzung der Rechte der Betroffenen
- Datenschutzvorfall
- Inspektion durch Aufsichtsbehörde (trifft vor allem spezielle Organisationstypen wie Banken und Versicherungen)

Rechte der Betroffenen

Müssen **fristgerecht** erfüllt werden können, dabei ist auf **Identitätsfeststellung** und **technische Umsetzbarkeit** zu achten:

- Informationspflicht, Auskunftsrecht
- Recht auf Löschung, Einschränkung und Datenübertragung
- Recht auf Berichtigung und Widerspruchsrecht

Verfahrensverzeichnis

Das Verzeichnis der Verarbeitungstätigkeiten protokolliert den Status Quo aller Datenanwendungen mit personenbezogenen Daten. **Neben** den **rechtlichen Mindestanforderungen** sollten im Rahmen der Erhebung **auch** alle weiteren Informationen erfasst werden, die zur Umsetzung der DSGVO benötigt werden (Auszug):

- Auflistung aller Verfahren und Datenkategorien plus Informationen zum Unternehmen
- Zwecke, Betroffene, Technisch-Organisatorische Maßnahmen, Rechtsgrundlagen
- Kategorien von Empfängern, Übermittlung in Drittländern, Löschfristen, Sensibilität

Wiederherstellung / Backup

Nach einem Schadensfall (z.B. technisches Gebrechen oder Cyberangriff) müssen Systeme und die dazugehörenden Informationen wiederhergestellt werden. Dafür braucht es ein:

- Backup-Konzept - **zeitlich** (wann werden Backups erstellt), **räumlich** (wo werden diese gespeichert, damit diese im Schadensfall erhalten bleiben z.B. Brand, Einbruch), **sachlich** (welche Daten werden gesichert)
- Wiederherstellungskonzept - **wer** (autorisierte und verfügbare Person), kann **was** (technische Infrastruktur) **wie** (Systemkonfiguration) mit **welchen** Informationen (Backups) wiederherstellen. Die Wiederherstellung sollte entsprechend getestet werden um sicherzustellen, dass Backup, Prozesse und Dokumentation ausreichend sind.

Checklist

Schritte zur Compliance - können Sie alle Anforderungen bis Mai 2018 erfüllen?

- Verfahrensverzeichnis
- Rechtsgrundlagen, Verträge und Informationspflichten
- Privacy by design / default
- Datenübermittlung ins Ausland
- Prozesse für Rechte der Betroffenen und Data Breach
- Datenschutz-Folgenabschätzung & Konsultation
- Datensicherheitsmaßnahmen / Technisch-Organisatorische Maßnahmen
- Datenschutzbeauftragter