EU-Datenschutz-Grundverordnung (DSGVO): Datensicherheitsmaßnahmen

Datensicherheit und Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen (Privacy by Design & Privacy by default)

Stand: 19.07.2018

Hinweis:
Die Bestimmungen der DSGVO und des österreichischen Datenschutzgesetzes (DSG) in der Fassung des Datenschutz-Anpassungsgesetzes 2018 und des Datenschutz-Deregulierungs-Gesetzes 2018 gelten seit 25.5.2018. Alle Datenverarbeitungen müssen dieser Rechtslage entsprechen. (Siehe dazu „Überblick")

Datensicherheit

Die Datensicherheit bei der Verarbeitung von personenbezogenen Daten soll in Zukunft noch effektiver gewährleistet werden.

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Dabei sind gegebenenfalls ua folgende Maßnahmen gefordert:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten (z.B. Passwortsicherungen von Dateien);
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen (z.B. Zutritts-/Zugangskontrollen, Zugriffsbeschränkungen). Dazu gehört auch, dass unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten („Auftragsprinzip");
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen (z.B. Backup-Programme);
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (z.B. Selbstevaluierungsprozesse).

Beurteilung des angemessenen Schutzniveaus:

Es sind die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere bei unbeabsichtigter oder unrechtmäßiger Vernichtung, Verlust, Veränderung, unbefugter Offenlegung oder unbefugtem Zugang zu personenbezogenen Daten („risikobasierter Ansatz“).

Die Einhaltung genehmigter Verhaltensregeln oder eines genehmigten Zertifizierungsverfahrens kann als Faktor herangezogen werden, um die Erfüllung der genannten Maßnahmen nachzuweisen.

Zum Schutz der personenbezogenen Daten haben die Verantwortlichen und die Auftragsverarbeiter ua auch die **Grundsätze des Datenschutzes durch Technik** (privacy by design) und durch **datenschutzfreundliche Voreinstellungen** (privacy by default) zu berücksichtigen und geeignete interne Strategien festzulegen sowie entsprechende Maßnahmen zu setzen.

Datenschutz durch Technik

Sowohl bei der Planung als auch bei der Datenverarbeitung selbst haben der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen zu berücksichtigen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Dabei sind der Stand der Technik, die Implementierungskosten, die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen (z.B. Pseudonymisierung).

Datenschutzfreundliche Voreinstellungen

Der Verantwortliche hat geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch entsprechende Voreinstellungen grundsätzlich nur solche personenbezogene Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

Die Einhaltung eines genehmigten Zertifizierungsverfahrens kann als Faktor herangezogen werden, um die Erfüllung der genannten Maßnahmen nachzuweisen.

Geldstrafen

Die Missachtung der Verpflichtung zu Datensicherheitsmaßnahmen sowie der Erfordernisse nach Datenschutz durch Technik und datenschutzfreundlichen Voreinstellungen ist mit bis zu EUR 10 Mio. oder 2% des letztjährigen weltweiten Jahresumsatzes sanktioniert.

Weitere Tipps zur konkreten Umsetzung siehe Website IT-SAFE.

Relevante Artikel der DSGVO: Art 25, Art 32

Relevante Erwägungsgründe: 75-79, 83-84