Datenschutzverordnung

Am 25. Mai 2018 ist das Datenschutzgesetz 2000 durch die EU-Datenschutz Grundverordnung (kurz: DSGVO) und das österreichische Datenschutzgesetz (kurz: DSG) ersetzt worden.

Die Datenschutz-Grundverordnung ist zwar als EU-Verordnung in jedem EU-Mitgliedstaat unmittelbar anwendbar, sie enthält jedoch zahlreiche Öffnungsklauseln und lässt dem nationalen Gesetzgeber gewisse Spielräume. Es gab daher auch in Österreich Novellen des österreichischen Datenschutzgesetzes 2000 (das „Datenschutz-Anpassungsgesetz 2018" und das „Datenschutz-Deregulierungsgesetz", beide nun im DSG enthalten). Seit 25. Mai 2018 müssen daher alle Datenanwendungen im Betrieb an die neue Rechtslage angepasst werden.

• Vereinzelt sind Unternehmen noch mit der Anpassung an die DSGVO und das DSG beschäftigt. Die WKO bietet hierzu eine Checkliste mit empfohlenen Schritten an, um ein Unternehmen datenschutz-fit zu machen.

Hinsichtlich Datensicherheit legt Artikel 32 der DSGVO sehr ähnlich zu den bisherigen Bestimmungen im DSG fest, dass 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 der Verantwortliche (vormals: datenschutzrechtlicher Auftraggeber) und der Auftragsverarbeiter (vormals: datenschutzrechtlicher Dienstleister) geeignete technische und organisatorische Maßnahmen treffen müssen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Darunter ist laut DSGVO folgendes zu verstehen:

• die Pseudonymisierung und Verschlüsselung personenbezogener Daten,

• die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen,

• die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,

• ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung,

• Sicherstellung, dass Mitarbeiterinnen und Mitarbeiter und sonstige unterstellte Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten.

Folgende Datensicherheitsmaßnahmen sind bereits bekannt (§ 14 DSG 2000) und finden in der Praxis durch folgende Maßnahmen statt:

• die ausdrückliche Festlegung der Aufgabenverteilung zwischen den Mitarbeiterinnen und Mitarbeitern;

• die Bindung der Datenverwendung an einen gültigen Auftrag z.B. eines oder einer Vorgesetzten;

• die Information und Schulung der Mitarbeiterinnen und Mitarbeiter über ihre Pflichten nach dem DSG und internen Datensicherheitsvorschriften;

• die Regelung der Zutrittsberechtigungen zu Räumen, in denen Daten verarbeitet werden;

• der Schutz der IT-Systeme und Datenträger vor unbefugten Zugriffen;

• der Schutz der IT-Systeme vor unbefugter Inbetriebnahme;

• die Protokollierung der Datenverwendung;

• die Dokumentation der oben angeführten Sicherheitsmaßnahmen in Form eines Datensicherheitshandbuchs.

Aus den Vorschriften des DSG ergeben sich nach wie vor einige typische Anforderungen für den Umgang mit personenbezogenen Daten: Alle Mitarbeiterinnen und Mitarbeiter müssen in Form einer Geheimhaltungsverpflichtung zum Datengeheimnis verpflichtet werden. Sie müssen geschult werden, typischerweise in Form von Seminaren oder Richtlinien. Aufgaben und Kompetenzen müssen durch Stellenbeschreibungen, Organisationshandbücher und andere

Anweisungen geregelt werden. Zutritts- und Zugriffsschutzmaßnahmen sowie Protokollierung müssen durch entsprechende, vorwiegend technische Einrichtungen gewährleistet sein.

Obwohl die Sicherheitsmaßnahmen der DSGVO bzw. des DSG an sich nur für die Verarbeitung personenbezogener Daten gelten, haben sie auch für die Verarbeitung anderer (nicht personenbezogener) Daten Bedeutung erlangt. Sie bilden eine Art Mindeststandard, der auch im Umgang mit Finanzdaten, Geschäftsgeheimnissen u.Ä. nicht unterschritten werden sollte.

Bei Datensicherheit spielt aber natürlich auch privacy by design und privacy by default eine Rolle. Privacy by design, oder Datenschutz durch Technikgestaltung, bedeutet, dass sowohl bei der Planung als auch bei der Datenverarbeitung selbst der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen zu berücksichtigen haben, 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).

Privacy by default, oder Privatsphäre durch geeignete Voreinstellungen, meint, dass der Verantwortliche geeignete technische und organisatorische Maßnahmen zu treffen hat, die sicherstellen, dass durch entsprechende Voreinstellungen grundsätzlich nur solche personenbezogenen 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.

Rolle des Datenschutzbeauftragten:

Der Datenschutzbeauftragte hat jedenfalls die folgenden Aufgaben zu erfüllen:

• Die Unterrichtung und Beratung der Unternehmer und Mitarbeiter hinsichtlich ihrer Pflichten nach dem Datenschutzrecht.

• Die Überwachung und Überprüfung der Einhaltung der Datenschutzvorschriften und Strategien für den Schutz personenbezogener Daten, einschließlich der Zuweisung von Zuständigkeiten, Sensibilisierung und Schulung der Mitarbeiter.

• Beratungen – auf Anfrage - im Zusammenhang mit der Überwachung ihrer Durchführung.

• Die Zusammenarbeit mit der Aufsichtsbehörde und Anlaufstelle für diese.

Qualifikationen:

An Qualifikationen muss der Datenschutzbeauftragte jedenfalls ein Fachwissen auf dem Gebiet des Datenschutzrechtes und der Datenschutzpraxis besitzen und die Fähigkeit die oben genannten Aufgaben zu erfüllen.

Aussageverweigerungsrecht:

Erhält ein Datenschutzbeauftragter bei seiner Tätigkeit Kenntnis von Daten, für die einer der Kontrolle des Datenschutzbeauftragten unterliegenden Stelle beschäftigten Person ein gesetzliches Aussageverweigerungsrecht zusteht, steht dieses Recht auch dem Datenschutzbeauftragten und den für ihn tätigen Personen insoweit zu, als die Person, der das gesetzliche Aussageverweigerungsrecht zusteht, davon Gebrauch gemacht hat.