EU-Datenschutz-Grundverordnung (DSGVO)

Überblick zum Datenschutz in Österreich

Am 4. Mai 2016 wurde die „Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)" kundgemacht.

Die **Datenschutz-Grundverordnung ist am 25. Mai 2018 in Geltung getreten**. Alle Datenverarbeitungen müssen dieser Rechtslage entsprechen.

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. Zur Durchführung dieser Öffnungsklauseln und Spielräume wurden in Österreich (neben Anpassungen in zahlreichen Materiengesetzen) zwei Novellen des Datenschutzgesetzes (das „Datenschutz-Anpassungsgesetz 2018" und das „Datenschutz-Deregulierungs-Gesetz 2018") beschlossen.[1]

Welche wesentlichen Neuerungen für Unternehmen enthält die Datenschutz-Grundverordnung (DSGVO)?

- Es gibt keine Meldepflicht bei der Datenschutzbehörde (Datenverarbeitungsregister) mehr.
- Statt dessen stärkere Verantwortung für Verantwortliche (derzeit „Auftraggeber") und Auftragsverarbeiter (derzeit „Dienstleister") und weitreichende Neuregelung der Pflichten bei der Datenverarbeitung:
  - Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen („privacy by design/privacy by default"): Es sind geeignete technische und organisatorische Maßnahmen und Verfahren (z.B. Pseudonymisierung) zu treffen, damit die Verarbeitung den Anforderungen der Verordnung genügt und die Rechte der betroffenen Personen geschützt werden. Datenschutzrechtliche Voreinstellungen sollen sicherstellen, dass grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.
  - Verantwortliche und Auftragsverarbeiter müssen ein „Verzeichnis von Verarbeitungstätigkeiten" führen: Der Inhalt ist ähnlich den derzeitigen DVR-Meldungen und hat insbesondere die eigenen Kontaktdaten, die Zwecke der Verarbeitung, eine Beschreibung der Datenkategorien und der Kategorien von betroffenen Personen, die Empfängerkategorien, gegebenenfalls Übermittlungen von Daten in Drittländer, wenn möglich die vorgesehenen Löschungsfristen und eine allgemeine Beschreibung der technischen und organisatorischen Datensicherheits-maßnahmen zu enthalten.
    Die Pflicht zur Führung dieses Verzeichnisses gilt für Unternehmen mit weniger als 250 Mitarbeitern - nur - dann nicht, wenn die von ihnen vorgenommene **Verarbeitung** kein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung **nur gelegentlich** erfolgt und keine Verarbeitung besonderer Datenkategorien bzw keine Verarbeitung von Daten über strafrechtliche Verurteilungen und Straftaten umfasst.
  - Verletzungen des Schutzes personenbezogener Daten sind sowohl den nationalen Aufsichtsbehörden (ohne unangemessene Verzögerung – möglichst binnen höchstens 72 Stunden nach dem Entdecken; außer die Verletzung führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten) als auch der betroffenen Person (ohne unangemessene Verzögerung, wenn die Wahrscheinlichkeit besteht, dass die Verletzung des Schutzes personenbezogener Daten ein hohes Risiko für die persönlichen Rechte und Freiheiten bewirkt) zu melden.
  - Pflicht zur Datenschutz-Folgenabschätzung bei Verarbeitungsvorgängen, die (insbesondere bei Verwendung neuer Technologien) aufgrund der Art, des Umfangs, der Umstände und der Zwecke voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben.
  - Vorherige Konsultation der Aufsichtsbehörde, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der für die Verarbeitung Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft.
  - (Verpflichtender) Datenschutzbeauftragter: Eine Verpflichtung zur Bestellung eines Datenschutzbeauftragten besteht für Unternehmen

(Verantwortliche und Auftragsverarbeiter), wenn
    - die Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen besteht, die aufgrund ihrer Art, ihres Umfanges und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Beobachtung von betroffenen Personen erforderlich machen, oder
    - die Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien von Daten oder von Daten über strafrechtliche Verurteilungen oder Straftaten besteht.

- (Neue) Informationspflichten und Betroffenenrechte
    - Informationen können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden
    - Informationen und Betroffenenrechte sind ohne unangemessene Verzögerung, spätestens aber innerhalb eines Monats zu erledigen (diese Frist kann um höchstens weitere 2 Monate verlängert werden)
    - Auskunftsrecht (ua auch über geplante Speicherdauer)
    - Recht auf Berichtigung
    - Recht auf Löschung und auf „Vergessenwerden"
    - Recht auf Einschränkung der Verarbeitung
    - Mitteilungspflicht bei Berichtigung, Löschung oder Einschränkung an alle Empfänger
    - Recht auf Datenübertragbarkeit
    - Widerspruchsrecht
    - Regelungen betreffend automatisierte Generierung von Einzelentscheidungen einschließlich profiling

- Befugnisse und Aufgaben der Aufsichtsbehörden werden erweitert
    - Insbesondere auch Verhängung von „Geldbußen"

- Hohe Strafen
    - Geldbußen von bis zu 20 Mio Euro oder im Fall eines Unternehmens von bis zu 4 % seines weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres.

---

[1] Der vierte Abschnitt des zweiten Hauptstücks (§§ 31-34) sowie das dritte Hauptstück (§§ 36-59) des Datenschutzgesetzes dienen der Umsetzung der Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. Nr. L119 vom 4.5.2016 S. 89.