Datenschutzverordnung

Von vielen Betrieben mit Vorsicht genossen oder streng beäugt tritt die EU-Datenschutz-Grundverordnung – kurz DSGVO genannt – ab 25. Mai 2018 in Kraft. Bis dahin müssen alle Datenanwendungen an die neue Rechtslage angepasst sein. Es herrschen große Unsicherheiten aufseiten der Kreativbetriebe, aber auch bei deren Kunden. Was ist zu tun? Worauf ist zu achten?

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 wurde in Österreich das „Datenschutz-Anpassungsgesetz 2018“, eine Novelle des DSG 2000 (künftig: DSG), beschlossen. Bis 24. Mai 2018 gelten die derzeitigen Regelungen des Datenschutzgesetzes 2000.

Neuerungen für Unternehmen
Es wird, so wie bisher, keine Meldepflicht bei der Datenschutzbehörde (Datenverarbeitungsregister) mehr geben. Die Verantwortlichen und Auftragsverarbeiter (Dienstleister) werden stattdessen mehr in die Pflicht genommen und es gibt 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 entspricht 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. Enthalten muss sein: die eigenen Kontaktdaten, die Verarbeitungszwecke, 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 Datensicherheitsmaßnahmen. Die Pflicht zur Führung dieses Verzeichnisses gilt für Unternehmen mit weniger als 250 Mitarbeitern. Ausgenommen sind Fälle, in denen 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 eingeschlossen ist.

Meldungen von Verletzungen des Schutzes personenbezogener Daten sind den nationalen Aufsichtsbehörden ohne unangemessene Verzögerung und das möglichst binnen höchstens 72 Stunden nach dem Entdecken mitzuteilen. Davon ausgenommen: Die Verletzung führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten. Zu informieren sind ebenso die betroffenen Personen ohne unangemessene Verzögerung, wenn die Wahrscheinlichkeit besteht, dass die Verletzung des Schutzes personenbezogener Daten ein hohes Risiko für die persönlichen Rechte und Freiheiten bewirkt.

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 zwei Monate verlängert werden).

Auskunftsrecht (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

Die **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 vier Prozent seines weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres.

Ablaufplan Datenschutz-Folgenabschätzung

Hier finden Sie eine Übersicht über die Prüfschritte kompakt zusammengefasst.

Checkliste – Prüfschritte

Prüfung, ob überhaupt die Voraussetzungen für die Durchführung einer verpflichtenden Datenschutz-Folgenabschätzung vorliegen
Erhebung der zu verarbeitenden personenbezogenen Datenarten (z. B. Namen, Adressen, Kontaktdaten, sensible Daten) und Feststellen der Rechtsgrundlage für die Datenverarbeitung
Werden die datenschutzrechtlichen Prinzipien eingehalten?
Darlegung der Gründe, warum eine Datenschutz-Folgenabschätzung für erforderlich bzw. für nicht erforderlich betrachtet wird (z. B. Bestehen einer Ausnahme gem. der „white list")
Konsultierung eines allenfalls bestellten betrieblichen Datenschutzbeauftragten
Beschreibung der geplanten Verarbeitungsvorgänge
Welche möglichen Risiken bestehen bei der beabsichtigten Datenverarbeitung für folgende Schutzziele (Datenverfügbarkeit, Integrität und Vertraulichkeit, Zweckbindung, sonstige Datenschutzprinzipien)?
Auf Basis der Identifizierung möglicher Risiken wird eine Risikoanalyse durchgeführt. Zunächst werden die möglichen Bedrohungen festgehalten (Von wem kann das Risiko ausgehen? Was könnten die Motive für die Bedrohung sein? Was könnte das mögliche Bedrohungsziel sein?). In weiterer Folge wird die Eintrittswahrscheinlichkeit des Risikos zu beurteilen sein und die daraus folgenden möglichen Folgen einer Risikoverwirklichung für die Betroffenenrechte.
Festhalten der bisher getroffenen Abhilfemaßnahmen: z. B. Anonymisierung oder Pseudonymisierung, Einsatz von Verschlüsselungstechnologien etc.
Aufstellung eines Maßnahmenplans: Auf Basis der bisherigen Prüfschritte können allfällige „Lücken" bei der Risikominimierung oder -behebung festgestellt werden, daraus sollte ein entsprechender Maßnahmenplan abgeleitet werden.

Weitere Informationen:
Checkliste
Kurzüberblick und Zeitplan
Ablaufplan und Prüfschritte

Foto: iStock.com/FroYo_92