Neue Pflichten, hohe Strafen – die EU-Datenschutz-Grundverordnung

Die EU-Datenschutz-Grundverordnung bringt eine Vielzahl an Neuerungen für Betriebe – was Sie wissen müssen.

Am 15.12.2015 konnten EU-Parlament, Rat und Kommission eine politische Einigung über die EU-Datenschutz-Grundverordnung (DSGVO) erzielen. Sie wird voraussichtlich ab dem 2. Quartal 2018 in ganz Europa direkt anwendbar sein und soll damit das Recht der Verwendung personenbezogener Informationen (Daten) vereinheitlichen. Die DSGVO enthält zahlreiche neue Pflichten für Auftraggeber von Datenanwendungen (zukünftig: Verantwortliche von Verarbeitungen) und wird Unternehmen eine höhere Eigenverantwortung bei der Datenverarbeitung verleihen, dafür aber auch eine viel dichtere Datenschutz-Compliance von ihnen verlangen. Verstöße gegen ihre Regelungen können drastische Strafen nach sich ziehen, können sie doch für Unternehmen bis max EUR 20 Mio oder 4 % des globalen Konzernumsatzes betragen! Unternehmen sind daher gut beraten, sich schnellstmöglich mit der DSGVO vertraut zu machen und Konformität ihrer Verarbeitungen von Kunden- und Mitarbeiterdaten sicherzustellen.

So erfahren etwa die Informationspflichten und die Betroffenenrechte eine deutliche Erweiterung. Letztere werden um das Recht auf Datenportabilität erweitert; ihnen wird bereits binnen Monatsfrist zu entsprechen sein. Generell sind Datenanwendungen nach Maßgabe von „Datenschutz durch Technik" und datenschutzfreundlichen Voreinstellungen zu konzeptionieren. Bei Datenverarbeitungen, die mit neuen Technologien arbeiten oder im Hinblick auf ihre Art oder Zwecke, ihren Anwendungsbereich oder Kontext als hohes Risiko für die Privatsphäre der Betroffenen erscheinen, ist zudem eine „Datenschutz-Folgeabschätzung" durchzuführen, die sogar eine Konsultation der Datenschutzbehörde erfordern kann.

„Unternehmen verlieren besser keine Zeit, um sich für die Anforderungen der DSGVO fit zu machen."

Die für die Datenverarbeitung Verantwortlichen und auch ihre Dienstleister werden ein Register der Verarbeitungstätigkeiten („Verfahrensverzeichnis") zu führen haben. Dieses muss die Zwecke einer Datenanwendung, die darin verarbeiteten Datenkategorien, die Kategorien von Empfängern, die Datensicherheitsmaßnahmen und die geplante Speicherdauer enthalten. Dienstleister müssen dieses Verzeichnis getrennt nach Auftraggebern führen.

Bei Datenmissbrauch oder -verlust muss zukünftig unverzüglich, soweit möglich, innerhalb von 72 Stunden nach Kenntnis die zuständige Datenschutzbehörde darüber informiert werden, außer der Vorfall birgt voraussichtlich kein Risiko für die Rechte und Freiheiten der Betroffenen. Wenn der Datenmissbrauch ein hohes Risiko für die Betroffenen bedeutet, müssen aber auch die Betroffenen unverzüglich verständigt werden.

Die DSGVO verpflichtet schließlich auch insbesondere große Unternehmen und jene, deren Kerngeschäft in der Verarbeitung personenbezogener Daten liegt, einen Datenschutzbeauftragten zu installieren. Dieser muss unabhängig sein, über ausreichende finanzielle Mittel verfügen, einschlägige Fachkenntnis und Erfahrung vorweisen können und direkt dem Vorstand berichtspflichtig sein.

Beschränkte Erleichterungen für international operierende Unternehmen kann das sogenannte One-Stop-Verfahren bringen, nach dem Verpflichtungen in Bezug auf transnationale Datenverarbeitungen durch mehrere Konzernunternehmen in unterschiedlichen Mitgliedstaaten bei der Datenschutzbehörde der Konzernhauptniederlassung erfüllt und erledigt werden können sollen.

In Anbetracht der Vielzahl an Neuerungen und der hohen Strafdrohung sollte keine Zeit verloren werden, um das Unternehmen für die Anforderungen der DSGVO fit zu machen.

Dr. Rainer Knyrim ist Rechtsanwalt und Partner bei Preslmayr Rechtsanwälte und schwerpunktmäßig im Datenschutzrecht tätig. Er ist Chefredakteur der Zeitschrift „Datenschutz konkret" (Verlag Manz).