



Sehr geehrte Damen und Herren,

Anfang Mai 2016 hat die Europäische Union (EU) die Endfassung der EU-Datenschutz-Grundverordnung (DS-GVO) veröffentlicht. Es steht damit fest, dass die DS-GVO ab dem 25.05.2018 unmittelbar in allen EU-Mitgliedsstaaten zu beachten ist und in ihrem Anwendungsbereich das derzeit geltende Bundesdatenschutzgesetz (BDSG) ersetzt. Die DS-GVO führt zu einer weitgehenden Vereinheitlichung des europäischen Datenschutzrechts. Sie bringt dabei im Vergleich mit der bisherigen Rechtslage in Deutschland erhebliche Veränderungen und Verschärfungen mit sich. Ergänzt wird sie durch das komplett neugefasste BDSG, das im Juli dieses Jahres im Bundesgesetzblatt verkündet wurde und das deutsche Datenschutzrecht an die Vorgaben der DS-GVO anpasst. Betroffen sind grundsätzlich alle Unternehmen, die personenbezogene Daten (z. B. Mitarbeiter- und/oder Kundendaten) verarbeiten. Wir möchten Ihnen mit dieser Praxisinfo einen kurzen Überblick über die wesentlichen Neuerungen und die hiermit verbundenen Herausforderungen für Unternehmen geben.

Für Fragen stehen Ihnen Ihre Ansprechpartner bei Kapellmann gerne zur Verfügung.

Ihr Kapellmann-Team

kapellmann.de/datenschutzrecht

Praxisinfo Datenschutzrecht: Die EU-Datenschutz-Grundverordnung (DS-GVO)

Die DS-GVO kommt. Unternehmen sind gut beraten, sich frühzeitig auf die neuen datenschutzrechtlichen Vorgaben einzustellen. Auch wenn bisher noch nicht alle Einzelfragen im Detail geklärt sind, ist schon jetzt offenkundig, dass insbesondere die Sanktionierung von Datenschutzverstößen deutlich verschärft wird. Die hiermit verbundenen Risiken lassen sich nur dann beherrschen, wenn rechtzeitig geeignete Datenschutz-Management-Systeme eingeführt werden.

Was ändert sich durch die DS-GVO?

Künftig werden Unternehmen erweiterte Nachweis- und Rechenschaftspflichten bzgl. ihrer Datenschutz-Maßnahmen treffen (sog. „Accountability“). Das Unternehmen trägt die Beweislast dafür, dass die Vorgaben der DS-GVO eingehalten werden. Darüber hinaus sieht die DS-GVO im Vergleich zur bisherigen Rechtslage deutlich umfassendere In-

formations- und Auskunftspflichten bei der Datenverarbeitung sowie strikere Löschpflichten vor.

Neu ist die sog. Datenschutz-Folgenabschätzung. Damit ist eine umfassende Vorprüfung gemeint, die durchzuführen und zu dokumentieren ist, wenn eine Datenverarbeitung hohe Risiken für die persönlichen Rechte der betroffenen Personen birgt. Davon ist insbesondere bei dem Einsatz neuer Verarbeitungsverfahren oder -technologien sowie bei der Verarbeitung großer Datenmengen oder besonders sensibler Daten auszugehen. Je nach Einzelfall kann zusätzlich eine Abstimmung mit der zuständigen Datenschutzbehörde erforderlich sein.

Die DS-GVO verlangt zudem von jedem Verantwortlichen, auf Basis einer Risikoanalyse ein angemessenes Datenschutzniveau durch Einführung geeigneter technischer und organisatorischer Maßnahmen vorzuhalten (Datenschutz-Compliance).

Dabei muss z.B. die Datenverarbeitung stets auf das für den Zweck der Verarbeitung notwendige Maß beschränkt sein (Datenminimierung). Dies ist u.a. durch sog. „datenschutzfreundliche Voreinstellungen“ zu gewährleisten. Außerdem bedarf es geeigneter Reaktionsmechanismen bei Datenschutzverstößen.

Auch die Regeln für die Auftragsverarbeitung werden verschärft. Insbesondere haften Auftragsverarbeiter künftig bei Datenschutzverstößen (neben dem Verantwortlichen) gegenüber geschädigten Personen auf Schadensersatz.

Was ändert sich durch das BDSG-Neu?

Die DS-GVO enthält eine Vielzahl von Öffnungsklauseln, die es den EU-Mitgliedstaaten erlauben, einzelne Bereiche durch eigene nationale Regelungen zu konkretisieren. Der deutsche Gesetzgeber hat auf dieser Grundlage das BDSG vollständig neugefasst. Das BDSG-Neu wird im Gleichlauf mit der DS-GVO am 25.05.2018 in Kraft treten. Es enthält u. a. Neuregelungen zum Beschäftigtendatenschutz und erhöhte Anforderungen an die Verarbeitung von sensiblen Daten. Darüber hinaus sieht das BDSG-Neu – neben weiteren Fällen – auch künftig eine Pflicht zur Bestellung eines Datenschutzbeauftragten für Unternehmen vor, die in der Regel mindestens 10 Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.

Was droht bei Verstößen?

Verstöße gegen die DS-GVO können gravierende Folgen haben: Es sind Bußgelder von bis zu 20 Mio. Euro oder – im Falle eines Unternehmens – von bis zu 4 Prozent des weltweiten (Konzern-) Umsatzes möglich, für die u. U. auch Geschäftsführer, verantwortliche Führungskräfte oder Datenschutzbeauftragte haftbar gemacht werden können. Selbst bei leichteren Verstößen kann ein Bußgeld von bis zu 10 Mio. Euro oder 2 Prozent des (Konzern-) Umsatzes drohen. Das BDSG-Neu sieht zudem unter bestimmten Voraussetzungen für Datenschutz-Verstöße eine Freiheitsstrafe von bis zu 3 Jahren vor. Hinzu kommt eine deutlich erweiterte zivilrechtliche Haftung, die auch zu immateriellen Schadensersatzverpflichtungen führen kann.

Was ist zu tun?

Das neue Datenschutzrecht wird aufgrund der Komplexität der Materie und des Zusammenspiels von DS-GVO, BDSG-Neu sowie Spezialregelungen auf europäischer und nationaler Ebene für Unternehmen ein gefährlicher „Paragrafen-Dschungel“.

Unternehmen müssen daher schon jetzt prüfen, wie sie die neuen datenschutzrechtlichen Anforderungen erfüllen können. In vielen Fällen wird es notwendig sein, vorhandene IT-Strukturen und geschäftliche Prozesse grundlegend neu zu bewerten und ggf. umzustellen, um Schadensersatz- und Bußgeldrisiken zu vermeiden. Dies erfordert eine sorgfältige Analyse des notwendigen Änderungsbedarfs sowie eine anschließende Planung, Implementierung und fortlaufende Überwachung der neuen Prozesse. Ziel muss es sein, ein für das Unternehmen angemessenes und effektives Datenschutzkonzept zu entwickeln und ein geeignetes Datenschutz-Management-System einzurichten.

Dabei kann es sinnvoll sein, auf vorhandene Compliance-Strukturen und -Ressourcen zurückzugreifen. Allerdings muss die Verantwortung für den Datenschutz grundsätzlich organisatorisch unabhängig sein, um mögliche Interessenkonflikte zu vermeiden. Insoweit sind zahlreiche klassische Compliance-Maßnahmen (z. B. Videoüberwachung, Whistleblowing, E-Searches) bereits nach geltendem Datenschutzrecht kritisch zu bewerten und bedürfen unter der DS-GVO und dem BDSG-Neu einer grundlegenden Neubewertung. Andernfalls kann Compliance schnell selbst zum Compliance-Fall werden.

Dies alles kostet Zeit. Die noch verbleibenden 5 Monate bis zur Geltung der neuen datenschutzrechtlichen Regelungen sollten daher gut genutzt werden. Dabei ist professionelle Rechtsberatung unerlässlich. Wir unterstützen Sie gerne dabei, Ihr Unternehmen auf das neue Datenschutzrecht vorzubereiten, insbesondere die notwendigen Strukturen und Prozesse zu identifizieren, zu entwickeln und zu implementieren.

Impressum

Alle Texte dieser Information sind urheberrechtlich geschützt. Gerne dürfen Sie Auszüge unter Nennung der Quelle nach schriftlicher Einwilligung durch uns nutzen. Obgleich diese Information sorgfältig erstellt wurde, wird keine Haftung für die Vollständigkeit und Richtigkeit übernommen. Sie soll einen ersten Überblick der angesprochenen Themen geben und stellt keinen anwaltlichen Rechtsrat dar. Sie ersetzt keine auf den Einzelfall bezogene Beratung. Wenn Sie unsere Praxisinfo nicht mehr erhalten möchten, können Sie diese unter newsletter@kapellmann.de abbestellen. © Kapellmann und Partner Rechtsanwälte mbB, Dezember 2017.