Europäische Datenschutzgrundverordnung

Die Europäische Datenschutzgrundverordnung (kurz: DSGVO) ist bereits am 24.05.2016 in Kraft getreten und ist für alle mit einer zweijährigen Übergangsfrist **ab 25.05.2018 geltendes Recht**. Die verbleibende Zeit bis Mai 2018 sollte von Unternehmen genutzt werden, um sich auf weitreichende Änderung im Datenschutzrecht einzustellen. Viele Maßnahmen erfordern eine gründliche Vorbereitungszeit, so dass für Unternehmen unmittelbar Handlungsbedarf besteht. Der Beitrag gibt einen Überblick über die wichtigsten Änderungen und enthält einen Fahrplan, an dem man sich orientieren kann.

Die wichtigsten Änderungen im Überblick

Das Wichtigste vorab: Ab dem 25.05.2018 wird von den Datenschutzaufsichtsbehörden erwartet, dass die Unternehmen die erforderlichen Maßnahmen zur Einhaltung der DSGVO umgesetzt zu haben. Da die Umstellungsfrist bereits läuft, ist mit einer weiteren Schonfrist nicht zu rechnen. Im Gegensatz zur jetzigen Rechtslage enthält die DSGVO bei einem Verstoß sehr empfindliche Geldbußen, die umsatzabhängig bis zu 20 Millionen Euro oder bis 4% vom Jahresumsatz betragen können. Diese Geldbußen können die Aufsichtsbehörden festsetzen, wenn ab dem 25.05.2018 keine oder nur unzureichende Vorbereitungen auf die DSGVO erfolgt sind. Zudem können auch Verbraucherschutzorganisationen und andere Verbände sowie Wettbewerber Datenschutzverstöße mit Abmahnungen verfolgen.

Datenpannen müssen binnen 72 Stunden gemeldet werden

Künftig muss jeder Datenschutzverstoß, der die Rechte und Freiheiten der Betroffenen beeinträchtigen könnte, innerhalb von 72 Stunden bei der zuständigen Aufsichtsbehörde und u.U. auch beim Betroffenen gemeldet werden. Unternehmen sollten Workflows einführen, um diese Pflicht innerhalb der kurzen Frist einhalten zu können.

Neue Informations- und Dokumentationspflichten

Mit der DSGVO werden zahlreiche weitere Informations- und Dokumentationspflichten eingeführt. Dazu gehört, dem Datenschutz schon bei der Produktentwicklung (privacy by design) und durch datenschutzfreundliche Voreinstellungen (privacy by default) Rechnung zu tragen. Neu eingeführt wird auch die sog. Datenschutzfolgenabschätzung: Bei Datenverarbeitungsvorgängen mit einem voraussichtlich hohen Risiko für personenbezogene Daten muss künftig geprüft werden, welche Folgen diese Risiken für den Schutz der personenbezogenen Daten haben.

Insbesondere: Verfahrensverzeichnisse

Von erheblicher Relevanz sind künftig sog. Verfahrensverzeichnisse, in dem die internen Prozesse bei der Verarbeitung personenbezogener Daten dokumentiert werden müssen. Diese müssen bis 25.05.2018 erstellt sein und auf Aufforderung der Aufsichtsbehörden vorgelegt werden können. Ansonsten drohen saftige Bußgelder. Verfahrensverzeichnisse sind zwar nicht neu und müssen schon nach bisherigem Recht erstellt werden. Sie werden als Compliance-Maßnahme nach der DSGVO künftig aber erheblich an Bedeutung zunehmen. Unternehmen, die bisher noch nicht damit gearbeitet haben, sollten diese nun rasch erstellen, da dies einiges an Vorbereitungszeit benötigt. Unter bestimmten engen Voraussetzungen sind kleine und mittlere Unternehmen KMU) mit weniger als 250 Mitarbeitern von dieser Pflicht nach Art. 30 Abs. 5 DSGVO befreit. Diese Ausnahmeregelung greift aber bereits dann nicht, wenn personenbezogene Daten regelmäßig verarbeitet werden wie dies typischerweise in der Finanzbuchhaltung, in der Personalabteilung oder in einer Kundendatenbank eines Unternehmens der Fall ist. Die allermeisten Unternehmen müssen somit Verfahrensverzeichnisse erstellen. Kleine Unternehmen bzw. Start-Ups könnten von der Ausnahmeregelung aber profitieren.

Die wichtigsten materiellen Änderungen im Überblick:

•Die Anforderungen an eine rechtswirksame Einwilligung der Betroffenen werden deutlich erhöht, z.B. wird das Kopplungsverbot verschärft. Das heißt, dass der Abschluss eines Vertrages nicht mehr von der Einwilligung abhängig gemacht werden darf, wenn dies für die Vertragsdurchführung nicht erforderlich ist (kein „take it or leave it“).

•Künftig wird es keine stillschweigende Einwilligung mehr geben. Eine Einwilligung ist künftig nur durch eine eindeutige Handlung möglich, z.B. durch aktives Setzen eines Häkchens auf einer Website.

•Die Anforderungen an den Widerruf einer Einwilligung werden erleichtert. Ein Widerruf ist künftig jederzeit und ohne Begründung möglich und muss mindestens so einfach gestaltet sein wie die Einwilligung selbst.

•Kinder und Jugendliche bedürfen bis zu einem Alter von 16 Jahren der Einwilligung der Eltern. Die EU-Mitgliedstaaten können das Mindestalter auf 13 Jahre herabsetzen. Unternehmen müssen die Einhaltung des Mindestalters dokumentieren und nachweisen.

•Da die Anforderungen an eine wirksame Einwilligung deutlich erhöht werden, müssen sich Unternehmen künftig auch darauf einstellen, die Verarbeitung personenbezogener Daten verstärkt auf den Erlaubnistatbestand „berechtigte Interessen“ zu stützen. Dies ist zu dokumentieren und auch in Datenschutzerklärungen umzusetzen.

•Auftragsdatenverarbeiter (künftig: Auftragsverarbeiter) werden verstärkt mit in die Verantwortung genommen. Er hat künftig eigene Dokumentationspflichten und haftet u.U. auch bei Datenpannen direkt gegenüber dem Betroffenen. Der Auftragsverarbeiter kann künftig bei Verstößen auch direkt zur Zahlung von Bußgeldern verpflichtet sein, etwa wenn kein schriftlicher Vertrag vorliegt. Auftragsverarbeiter müssen künftig auch die Verarbeitungsvorgänge dokumentieren, d.h. u.U. Verfahrensverzeichnisse führen.

•Informations- und Auskunfts- und Löschpflichten der Unternehmen werden erweitert, Dokumentationspflichten erhöht. Künftig muss in jedem Einzelfall dokumentiert sein, wann welche personenbezogene Daten wie verarbeitet werden und auf welcher Rechtsgrundlage dies erfolgt. Darüber muss dem Betroffenen jederzeit Auskunft gegeben werden können.

•Der Betroffene hat künftig ein Recht auf Datenportabilität. Dafür müssen die technischen Voraussetzungen geschaffen werden, z.B. auf Anfrage die Übermittlung von Daten in ein transportfähiges Format an den Betroffenen oder an Dritte. Dies ist vor allem für Anbieter sozialer Netzwerke bedeutsam.

Fahrplan bis Mai 2018

Die wichtigsten Maßnahmen bis Mai 2018 sind:

•Prüfung, ob Verfahrensverzeichnisse erstellt werden müssen; bejahendenfalls muss damit rasch begonnen werden.

•Überprüfung von AGBs / sonstigen Nutzungsbedingungen auf Websites.

•Anpassung der Workflows und Unternehmensprozesse bei der Verarbeitung personenbezogener Daten.

•Einwilligungserklärungen im Netz sind auf Wirksamkeit und Transparenz zu überprüfen, Widerrufe technisch zu erleichtern, vor allem auf Websites, Apps und anderen digitalen Diensten.

•Prüfung, ob nach neuem Recht eine Verpflichtung zur Benennung eines Datenschutzbeauftragten besteht.

•Dokumentation aller Datenverarbeitungsprozesse als Basis für die Anpassung an DSGVO-Vorgaben.

•Anpassung von Datenschutzerklärungen und Verträgen zur Auftragsdatenverarbeitung.

•Schaffung von Unternehmensprozessen, um bei Datenschutzverletzungen die 72-Stunden-Frist einhalten zu können.

Betroffen sind praktisch alle Unternehmen, die personenbezogene Daten (auch ihrer Beschäftigten) verarbeiten. Da bereits fast ein Jahr von der Umstellungsfrist abgelaufen ist, ist Eile geboten, um den Fahrplan für die Umsetzung der erforderlichen Anpassungen an die DSGVO noch einhalten zu können.

Datenschutzbeauftragter

Es sollte auch geprüft werden, ob ein Datenschutzbeauftragter bestellt werden muss. Schon nach jetziger Rechtslage muss ein betrieblicher Datenschutzbeauftragter in Unternehmen mit mehr als 9 Beschäftigten bestellt werden, wenn regelmäßig personenbezogene Daten automatisiert verarbeitet werden, was schon dann der Fall ist, wenn Beschäftigte mit Externen per E-Mail kommunizieren. Aber auch kleine Unternehmen bzw. Start-ups mit weniger als 9 Beschäftigten müssen nach neuem Recht unter bestimmten Voraussetzungen künftig einen Datenschutzbeauftragten benennen, z.B. wenn personenbezogene Daten als Haupttätigkeit verarbeitet werden. Dabei wird vertreten, dass eine Haupttätigkeit schon dann vorliegt, wenn ein kleiner Onlineshop-Betreiber für die Verbesserung seines Webangebotes Nutzerdaten auswerten lässt. Der Datenschutzbeauftragte kann auch ein Externer sein, z.B. ein Rechtsanwalt. Wegen der künftigen erhöhten Anforderungen und Risiken nach der DSGVO empfiehlt sich als Compliance-Maßnahme, freiwillig einen Datenschutzbeauftragten zu ernennen, auch wenn keine Verpflichtung bestehen sollte.