Neue EU-Datenschutzgrundverordnung: Auswirkungen für Unternehmen

Seit dem 25. Mai 2018 gilt die neue EU-Datenschutzgrundverordnung (DSGVO), die in allen Mitgliedsstaaten unmittelbar gilt. Zeitgleich mit der DSGVO ist das neue Bundesdatenschutzgesetz in Kraft getreten, das die DSGVO zum Teil modifiziert und konkretisiert. Was müssen deutsche Unternehmen nunmehr aufgrund der DSGVO und den neuen deutschen Datenschutzregelungen beachten?

Die DSGVO und das neue Bundesdatenschutzgesetz haben erhebliche Auswirkungen auf die Zulässigkeit der Verarbeitung personenbezogener Daten. Sie gelten sowohl für Ein-Personen-Unternehmen als auch für Konzerne. Unternehmen müssen nun in größerem Umfang als bisher gegenüber den Betroffenen über die durch sie gespeicherten Daten Auskunft erteilen. So haben Betroffene etwa das Recht von den Verantwortlichen eine Bestätigung darüber zu verlangen, ob personenbezogene Daten von ihnen zu welchem Zweck verarbeitet werden. Die Erhebung und Verarbeitung persönlicher Daten darf nur mit einer vorherigen eindeutigen Einwilligung des Betroffenen erfolgen. Nur in gesetzlich geregelten Fällen kann auf die Einwilligung verzichtet werden. Zusätzlich zum Auskunftsrecht erhalten die Betroffenen auch das Recht von dem Verantwortlichen eine kostenlose Kopie aller verarbeiteten Daten zu verlangen. Ferner besteht das Recht

- auf Berichtigung unrichtiger oder Vervollständigung der gespeicherten personenbezogenen Daten,
- auf Löschung,
- auf Einschränkung der Verarbeitung,
- auf Widerspruch,
- auf Beschwerde bzgl. der Herkunft der Daten sowie
- auf Information über das Bestehen einer automatisierten Einzelfallentscheidung einschließlich Profiling (z.B. das Erstellen eines umfassenden Nutzerprofils oder die Bildung von sog. Scorewerten durch Verknüpfen, Speichern, Auswerten und Zusammenlegen von verschiedenen Daten zu einer Person) und ggf. darüber, ob die automatisierte Entscheidung z.B. gesetzlich bzw. vertraglich vorgeschrieben oder für einen Vertragsschluss erforderlich ist.

Betroffene werden durch das neu etablierte Recht auf Datenübertragbarkeit zudem befugt, ihre Daten „*mitzunehmen*“. Das bedeutet, dass sie einen Verantwortlichen anweisen können,

gewisse Daten von einer automatisierten Anwendung (etwa einem sozialen Netzwerk) auf eine andere Anwendung zu übertragen. Als besondere Ausformung des Löschungsrechts beim Online-Händler gibt es ein „*Recht auf Vergessenwerden*“. Die Änderung bezieht sich insbesondere auf die Anzeige der personenbezogenen Daten in Suchmaschinen.

Die DSGVO sieht darüber hinaus vor, dass bei solchen privaten Stellen, deren Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen liegt, welche etwa eine regelmäßige und systematische Überwachung von betroffenen Personen in großem Umfang erforderlich machen, ein Datenschutzbeauftragter zu bestellen ist. Das neue Bundesdatenschutzgesetz enthält konkrete Vorgaben, wann die Pflicht zur Bestellung eines Datenschutzbeauftragten besteht, nämlich

- wenn in der Regel mindestens 10 Personen selbständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt werden,
- die Verarbeitung eine Datenschutzfolgenabschätzung erforderlich macht,
- personenbezogene Daten geschäftsmäßig zum Zwecke der Übermittlung oder
- der Markt- oder Meinungsforschung verarbeitet werden.

Der Datenschutzbeauftragte kann sowohl Mitarbeiter des datenverarbeitenden Unternehmens, als auch ein Externer sein, sofern dies nicht zu einem Interessenkonflikt führt. Wichtig ist in diesem Zusammenhang, dass die Bestellung eines Datenschutzbeauftragten kein „*Freibrief*“ ist, sondern die Geschäftsführung des datenverarbeitenden Unternehmens nach außen weiterhin haftet, auch für Mitarbeiter-Fehlverhalten.

Vollkommen neu ist, dass Unternehmen eine sogenannte Datenschutzfolgenabschätzung erstellen müssen. Diese ist immer dann durchzuführen, wenn ein Datenverarbeitungsverfahren voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen birgt, etwa durch neue Technologien, die automatisiert, systematisch und umfassend Daten erfassen, verarbeiten und bewerten. Die Datenschutzfolgeabschätzung hat etwa eine systemtische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung sowie die Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge zu enthalten. Kommt das Unternehmen bei ihrer Bewertung zu dem Ergebnis, dass trotz des Eingreifens technischer und organisatorischer Maßnahmen ein hohes Risiko für die Rechte und Freiheiten der Betroffenen verbleibt, hat es die Aufsichtsbehörde zu konsultieren. Diese kann dann innerhalb von 8 Wochen Empfehlungen aussprechen.

Die DSGVO sieht eine Reihe von Bußgeldtatbeständen vor. Je nach Schwere des Verstoßes können nunmehr Bußgelder bis zu € 20 Mio. oder 4 % des weltweiten Firmenjahresumsatzes (der jeweils höhere Betrag wird angesetzt) gegen Unternehmen verhängt werden. Zusätzlich gibt die DSGVO den Mitgliedsstaaten den Auftrag, Sanktionen für Verstöße festzulegen, die in ihr selbst nicht geregelt sind. Entsprechend sieht das neue Bundesdatenschutzgesetz Strafvorschriften vor, die erhebliche praktische Bedeutung erlangen können. Sie greifen beispielsweise dann ein, wenn es um Daten einer „*großen Zahl von Personen*“ geht, die in gewerbsmäßiger Weise unzulässig an einen Dritten übermittelt werden. Dafür ist eine Freiheitsstrafe bis zu 3 Jahren vorgesehen.

Fazit: In der Praxis wird die Umsetzung der Vorgaben des DSGVO sowie des neuen Bundesdatenschutzgesetzes neue datenschutzrechtliche Prozesse erforderlich machen. Hierzu wird für Unternehmen ein wichtiger Schritt sein, entsprechende Compliance-Regeln aufzustellen, die den richtigen Umgang ihrer Mitarbeiter mit personenbezogenen Daten festlegen und geeignete technische und organisatorische Maßnahmen zu ergreifen, um sicherzustellen und den Nachweis dafür zu erbringen, dass die Datenverarbeitung in Übereinstimmung mit der DSGVO erfolgt. Nur so kann eine Enthaftung der Geschäftsführung gelingen. Sonst drohen im Extremfall immense Bußgelder.

Dr. Thanh-Thuy Du-Quoc