Die EU-Datenschutz-Grundverordnung in Unternehmen

Aufgaben und Pflichten der Unternehmen

Im Zuge der EU-Datenschutz-Grundverordnung werden die Aufgaben und Pflichten der Unternehmen erweitert, um den Schutz personenbezogener Daten umfassend zu gewährleisten. Dieser Beitrag soll einen Überblick über die wichtigsten und nicht abschließend aufgezählten Anforderungen an Unternehmen verschaffen und deren neue Organisationspflichten kurz skizzieren. Bis zur verbindlichen Anwendung ab dem 25.05.2018 sollten Unternehmen zur Vermeidung der empfindlichen Bußgelder die Vorgaben der Verordnung umsetzen.

Foto: Henseler & Partner

Rechtsanwältin Bahar Beyaz,
Henseler & Partner Rechtsanwälte mbB

Nach dem Transparenzgebot der Datenschutz-Grundverordnung (DS-GVO) müssen Unternehmen künftig betroffene Personen wesentlich umfassender als bisher über den Umfang der Verarbeitung ihrer personenbezogenen Daten informieren. Bereits bei Erhebung der Daten sind diese Informationen den betroffenen Personen mitzuteilen.

Bei diesen Informationen handelt es sich unter anderem um die Kontaktdaten des Verantwortlichen, also des datenverarbeitenden Unternehmens, die Zwecke und die Rechtsgrundlage der Verarbeitung der personenbezogenen Daten, deren Speicherdauer, die Rechte der Betroffenen, die ggfs. geplante Übermittlung der personenbezogenen Daten an Drittländer, die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und die Kontaktdaten des Datenschutzbeauftragten.

Die genannten Informationen sind grundsätzlich in Schriftform oder elektronischer Form zu verfassen. Daher sind solche Informationen auf einer Homepage des Unternehmens zwingend bereitzuhalten. Es hat sich in der Praxis durchgesetzt, solche Informationen in einer Datenschutzerklärung zusammenzufassen. Unternehmen sollten somit überprüfen, ob sie auf ihrer Webseite eine Datenschutzerklärung bereithalten und ob diese den Anforderungen der DS-GVO entsprechen.

Anlegen einer Verarbeitungsübersicht

Nach der DS-GVO sind Unternehmen außerdem zum Führen einer Verarbeitungsübersicht verpflichtet. Die hierdurch erfolgte Bestandsaufnahme über die personenbezogenen Daten und deren Verarbeitung ermöglicht eine Gesamtbetrachtung und die Sicherung der Gesetzeskonformität. Außerdem wird bei einem Datenschutz-Audit die Nachvollziehbarkeit der Verarbeitung von personenbezogenen Daten wesentlich erleichtert.

Von dieser Pflicht nicht betroffen sind Unternehmen mit weniger als 250 Mitarbeitern, sofern die Datenverarbeitung kein Risiko für Rechte und Freiheiten der Betroffenen birgt oder die Datenverarbeitung nur gelegentlich erfolgt oder keine besonderen Arten personenbezogener Daten verarbeitet werden.

Zuständig für die Erstellung und Führung einer Verarbeitungsübersicht ist stets die Unternehmensleitung, nicht ein interner oder externer Datenschutzbeauftragter.

Eine Verarbeitungsübersicht sollte schriftlich oder in elektronischer Form angelegt werden. Empfehlenswert ist die elektronische Form, so dass diese ggfs. der Aufsichtsbehörde oder dem Betroffenen übersandt werden kann.

Die in die Verarbeitungsübersicht aufzunehmenden Angaben sind: Name und Kontaktdaten der Unternehmen, die Zwecke der Verarbeitung, die Kategorien betroffener Personen und personenbezogener Daten, die Kategorien von Datenempfängern, die Übermittlung in Drittländer, Löschfristen für die personenbezogenen Daten sowie Angaben zur Datensicherheit.

Erste Mustervorlagen einer Verarbeitungsübersicht sind auf den Webseiten einiger Aufsichtsbehörden – der Landesdatenschutzbeauftragten – abrufbar.

Datenschutzfolgenabschätzung

Gänzlich neu eingeführt wird durch die DS-GVO die Datenschutzfolgenabschätzung. Hierbei handelt es sich um ein Instrument zur Erkennung von Risiken, die mit der Verarbeitung von personenbezogenen Daten entstehen und die Rechte und Freiheiten der betroffenen Personen gefährden könnten. Ziel ist es, insbesondere die Eintrittswahrscheinlichkeit und Schwere der möglichen Risiken zu bewerten. Die Folgen von Datenverarbeitungsvorgängen sollen möglichst umfassend erfasst werden. Dabei sollen auch Maßnahmen und Verfahren geprüft werden, die solche Risiken mit adäquaten

Gegenmaßnahmen verringern könnten. Mögliche Risiken für betroffene Personen sind beispielsweise materielle/immaterielle Schäden, Diskriminierung, Identitätsdiebstahl oder -betrug, Rufschädigung, etc.

Indizien für die Notwendigkeit einer Datenschutzfolgenabschätzung sind die Verwendung neuer Technologien, neuartige Verarbeitungsvorgänge, umfangreiche Verarbeitungsvorgänge, Verarbeitung sensibler Daten, Profiling, systematische und öffentliche Überwachung etc.

Im Falle eines Unterlassens der Durchführung einer vorgeschriebenen Datenschutzfolgenabschätzung oder der Durchführung in nicht vorgegebener Weise kann die zuständige Aufsichtsbehörde dies mit Bußgeldern ahnden.

Bestellung eines Datenschutzbeauftragten

Auch die Bestellung eines Datenschutzbeauftragten, der künftig über eine wichtigere Stellung im Unternehmen verfügen wird, gehört zu den bedeutenden Pflichten der Unternehmen. Die Einzelheiten hierzu wurden bereits im Stahlreport 12/17 dargelegt.

Schaffung von technischen und organisatorischen Maßnahmen

Die Schaffung von technischen und organisatorischen Maßnahmen soll durch die Implementierung von angemessenen Sicherheitsstandards erfüllt werden. Insbesondere soll hierdurch ein unzulässiger Umgang mit personenbezogenen Daten verhindert und die Integrität und Verfügbarkeit dieser Daten gewährleistet werden.

Beispiel für technische Maßnahmen ist die Einhaltung des Standes der Technik, die Pseudonymisierung oder Verschlüsselung von personenbezogenen Daten und die Einrichtung technischer Zugriffsrechte. Als Beispiel für organisatorische Maßnahmen ist die Beaufsichtigung von Personal, das Zugang zu personenbezogenen Daten hat, die Einrichtung physischer Zutritts, Zugriffs- oder Zugangskontrollen, die entsprechende Personalplanung, die Minimierung der Verarbeitung von personenbezogenen Daten und die regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit technischer und organisatorischer Maßnahmen zur Umsetzung zu nennen.

Die Einhaltung der genannten Maßnahmen ist im Falle eines Datenschutzverstoßes ein wichtiges Kriterium für die Aufsichtsbehörden, ob und in welcher Höhe ein Bußgeld verhängt wird. Eine strenge und gut dokumentierte Beachtung kann demnach zur erheblichen Schadensminimierung führen.

Meldepflichten bei Datenpannen

Die DS-GVO schreibt Unternehmen eine unverzügliche Meldepflicht bei den zuständigen Aufsichtsbehörden im Falle einer Datenpanne vor. Hierunter fällt „eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder rechtmäßig, zur Vernichtung, zum Verlust oder zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang an personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden".

Die Aufsichtsbehörden sind grundsätzlich innerhalb von 72 Stunden nach Bekanntwerden der Datenpanne zu benachrichtigen. Diese Pflicht entfällt, wenn voraussichtlich kein Risiko für die Rechte und Freiheiten der betroffenen Personen besteht. Die Meldung unterliegt zwingenden inhaltlichen Anforderungen. Bei einem hohen Risiko eines Schadenseintritts ist auch die betroffene Person selbst von der Datenpanne zu informieren.

Fazit

Wie den zuvor dargelegten und nicht abschließend aufgeführten Pflichten zu entnehmen ist, kommen auf Unternehmen zahlreiche und vielfältige neue Aufgaben zu. Wie dies in der Praxis tatsächlich umgesetzt werden soll, ist bislang noch völlig offen.

In jedem Fall sollten insbesondere die zuständigen Mitarbeiter durch Schulungen auf das Thema sensibilisiert werden, um ein Bewusstsein für den sorgsamen Umgang mit personenbezogenen Daten hervorzurufen. Darüber hinaus sollten bestehende Auftragsdatenverarbeitungsverträge entsprechend angepasst und für unsichere Sachlagen notfalls neu aufgesetzt werden.

Ratsam ist auch eine Art „Notfallplan", der im Falle einer Datenpanne greifen soll. In Anbetracht der weiterhin bestehenden großen Rechtsunsicherheit und der noch ausstehenden praktischen Handhabung der Vorgaben der DS-GVO sollten die Meldungen der Aufsichtsbehörden verfolgt und deren Praxisleitfäden zur unternehmenseigenen Umsetzung herangezogen werden.

Schließlich soll an dieser Stelle auch nochmals auf die Wichtigkeit einer einwandfreien Datenschutzerklärung erinnert werden. Diese gilt als „Achillesverse", da Konkurrenzunternehmen und auch Aufsichtsbehörden über die Unternehmenswebseite auf diese jederzeit zugreifen und dessen Defizite erkennen können. Zur Verringerung der „Verwundbarkeit" ist daher dessen Überprüfung und Anpassung unerlässlich.

INFO

Ab dem 25.05.2018 gilt in der Europäischen Union die Datenschutzgrundverordnung (DS-GVO) und enthält strengere Bestimmungen und Vorgaben für den Umgang der Unternehmen mit personenbezogenen Daten ihrer Mitarbeiter und Kunden. Im Zuge der Reform wird auch das noch geltende Bundesdatenschutzgesetz (BDSG) durch das neue Bundesdatenschutzgesetz (BDSG-neu) ersetzt, welches die genannte Verordnung ergänzt. Die E-Privacy-Verordnung, ebenfalls ab dem 25.05.2018 geltend, soll an die DS-GVO anknüpfen und deren Regelungsbereich spezifisch für die Nutzung elektronischer Kommunikationsdienste und -vorgänge komplettieren.

Anlässlich der Reformierung des Datenschutzrechtes ab Mai 2018 sollen die wichtigsten Änderungen und damit einhergehenden praktischen Anforderungen in Unternehmen in der Reihe „Die EU-Datenschutz-Grundverordnung in Unternehmen" von Rechtsanwalt Dr. Thorsten Hauröder und Rechtsanwältin Bahar Beyaz von Henseler & Partner Rechtsanwälte mbB dargestellt werden.