ComplianceBusiness
Ausgabe 2 // Juni 2018

Wirksam, verhältnismäßig, abschreckend

Im Blickpunkt: Die Bußgeldvorschriften nach der EU-Datenschutz-Grundverordnung

Von Barbara Scheben

Ein wirksames Datenschutzmanagementsystem ist fortan essentieller Bestandteil der unternehmerischen Governance.

Seit dem 25.05.2018 ist die EU-Datenschutz-Grundverordnung in allen EU-Mitgliedstaaten unmittelbar anwendbar. Sie gilt teilweise auch über die Grenzen der EU hinaus, soweit einer Person in der Union Waren oder Dienstleistungen angeboten werden oder ihr Verhalten in der Union beobachtet wird. In Deutschland wird die DSGVO flankiert durch das neue Bundesdatenschutzgesetz (BDSG). In beiden Vorschriften finden sich neue Bußgeldregelungen, mit denen jedes Unternehmen vertraut sein sollte.

Neue Anforderungen an die Datenschutzorganisation

Die DSGVO bringt zahlreiche neue Anforderungen an die Datenschutzorganisation im Unternehmen mit sich, welche die Einrichtung eines Datenschutzmanagementsystems erfordern. Risikoanalyse, Transparenz und Dokumentation sind zentrale Anforderungen. Der Erfüllung der Betroffenenrechte kommt maßgebliche Bedeutung zu. Der Verantwortliche ist für die Einhaltung der Vorgaben der DSGVO verantwortlich und muss dies nachweisen können („Rechenschaftspflicht“).

ComplianceBusiness
Ausgabe 2 // Juni 2018

Höhe der Geldbußen

Die DSGVO sieht Geldbußen von insgesamt bis zu 20 Millionen Euro oder im Fall eines Unternehmens von bis zu 4% seines gesamten weltweit erzielten Vorjahresumsatzes vor. Zu berücksichtigen ist, dass der Begriff des „Unternehmens" im Sinne der Art. 101 und 102 AEUV (Vertrag über die Arbeitsweise der Europäischen Union) zu verstehen ist und somit die „wirtschaftliche Einheit" als Ganzes erfasst. Der Datenschutzverstoß einer kleinen Tochtergesellschaft kann also mit Blick auf den Konzernumsatz als Bemessungsgrundlage enorme Wirkung haben. Adressat der Bußgeldvorschriften der DSGVO sind der Verantwortliche und der Auftragsverarbeiter.

Geldbußen von bis zu 10 Millionen Euro oder bis zu 2% des gesamten weltweit erzielten Vorjahresumsatzes werden unter anderem verhängt bei Verstößen gegen die Pflichten der Verantwortlichen oder der Auftragsverarbeiter gemäß den Art. 8, 11, 25–39, 42 und 43 DSGVO. Außerdem bei Verstößen gegen die Pflichten der Zertifizierungsstelle gemäß den Art. 42 und 43 DSGVO sowie die Pflichten der Überwachungsstelle gemäß Art. 41 Abs. 4 DSGVO. Relevant werden danach insbesondere Verstöße mit Blick auf die Anforderungen an das Datenschutzmanagementsystem. Bebußt werden etwa die Nichteinhaltung der Vorgaben an die Auftragsverarbeitung, das Unterlassen der Führung eines Verarbeitungsverzeichnisses, das Nichteinrichten geeigneter technischer und organisatorischer Maßnahmen zur Datensicherheit, die Nichtdurchführung einer Datenschutzfolgenabschätzung sowie Mängel und Unterlassen im Umgang mit Datenschutzverstößen im Zusammenhang mit der Meldung an die Aufsichtsbehörde und der Benachrichtigung der Betroffenen. Auch die Verletzung der Vorgaben im Zusammenhang mit der Bestellung und Aufgabenwahrnehmung durch den Datenschutzbeauftragten fallen in diese Kategorie.

Geldbußen von bis zu 20 Millionen Euro oder bis zu 4% des gesamten weltweit erzielten Vorjahresumsatzes werden insbesondere verhängt bei Verstößen gegen die sogenannten Grundsätze der Verarbeitung. Diese finden sich in Art. 5 DSGVO und beinhalten die Grundsätze der Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit einschließlich der Bedingungen für die Einwilligung gemäß der Art. 5, 6, 7 und 9 DSGVO sowie bei Verstößen gegen die Rechte der Betroffenen gemäß den Art. 12–22 DSGVO. Hierzu zählen vor allem die Informationspflicht, das Recht auf Auskunft, das Recht auf Berichtigung, das Recht auf Löschung, das Recht auf Datenübertragbarkeit sowie das Widerspruchsrecht. Die DSGVO sieht in den genannten Artikeln weitere Betroffenenrechte vor. Ebenso in diese Kategorie fallen Verstöße im Zusammenhang mit den Vorgaben der DSGVO zur Drittstaatenübermittlung, Verstöße gegen Pflichten gemäß den Rechtsvorschriften der Mitgliedstaaten, wie etwa die Vorgaben des § 26 BDSG zur Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses, sowie die Nichtbefolgung bestimmter Anweisungen der Aufsichtsbehörde.

Verstoßen ein Verarbeitungsvorgang oder mehrere miteinander verbundene Verarbeitungsvorgänge gegen mehrere Vorschriften der DSGVO, wird eine Gesamtgeldbuße festgesetzt. Diese darf jedoch den Betrag für den schwerwiegendsten Verstoß nicht übersteigen.

Leitplanken für die Bußgeldbemessung

Nach den Vorgaben der DSGVO sollen die verhängten Geldbußen „in jedem Einzelfall wirksam, verhältnismäßig und abschreckend" sein. Sie gibt außerdem Leitplanken für die Bußgeldbemessung vor, die auch für Unternehmen nützliche Hinweise enthalten. So hat die Aufsichtsbehörde bei der Bebußung in jedem Einzelfall folgende Aspekte zu berücksichtigen:

- Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens;

- Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;

- jegliche von dem Verantwortlichen oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens;

- Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß den Art. 25 und 32 getroffenen technischen und organisatorischen Maßnahmen;

- etwaige einschlägige frühere Verstöße des Verantwortlichen oder des Auftragsverarbeiters;

ComplianceBusiness
Ausgabe 2 // Juni 2018

- Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern;

- Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind;

- Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang der Verantwortliche oder der Auftragsverarbeiter den Verstoß mitgeteilt hat;

- Einhaltung der nach Art. 58 Abs. 2 früher gegen den für den betreffenden Verantwortlichen oder Auftragsverarbeiter in Bezug auf denselben Gegenstand angeordneten Maßnahmen, wenn solche Maßnahmen angeordnet wurden;

- Einhaltung von genehmigten Verhaltensregeln nach Art. 40 oder genehmigten Zertifizierungsverfahren nach Art. 42 und

- jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste.

Zielsetzung der DSGVO: Compliance soll sich lohnen

Hier kommt die Wirkung des gelebten Datenschutzmanagements entscheidend zum Tragen. Prävention, Proaktivität und Kooperation können sich bußgeldmindernd auswirken. Die DSGVO zeigt sich sehr modern und übernimmt den Gedanken, der schon aus dem internationalen Korruptionsstrafrecht bekannt ist: Compliance soll sich lohnen.

Neben den Bußgeldvorschriften der DSGVO sind diejenigen des BDSG zu beachten (siehe §§ 30 und 43 BDSG). Hier finden sich Sondervorschriften im Zusammenhang mit Verbraucherkrediten. Der Vollständigkeit halber sei erwähnt, dass das BDSG außerdem Strafvorschriften enthält. Zudem erklärt § 41 BDSG insbesondere die Vorschriften der §§ 30, 130 des Gesetzes über Ordnungswidrigkeiten für anwendbar.

Neben den bußgeldrechtlichen Folgen können Datenschutzverstöße zudem administrative Maßnahmen der Aufsichtsbehörde wie auch Schadensersatzforderungen für materielle und immaterielle Schäden nach sich ziehen. Aufgrund all dieser teilweise drastischen Folgen ist ein wirksames Datenschutzmanagementsystem fortan essentieller Bestandteil der unternehmerischen Governance.

Barbara Scheben,
Rechtsanwältin, Partner, Compliance & Forensic, KPMG AG Wirtschaftsprüfungsgesellschaft, Frankfurt am Main

bscheben@kpmg.com
www.kpmg.de/forensic