30.04.2018 von Nils Steffen (Kommentare: 0)

EU-Datenschutzgrundverordnung

von Rechtsanwalt Nils Steffen

Ab dem 25.05.2018 ist die Datenschutz-Grundverordnung (DS-GVO) anzuwenden und regelt ab diesem Tag den Datenschutz innerhalb der Europäischen Union neu. Die DS-GVO trat am 25.05.2016 in Kraft und sieht eine zweijährige Transformationszeit vor. Die Unternehmen sollten dadurch die Gelegenheit erhalten ihre Datenverarbeitungsprozesse bezüglich personenbezogener Daten an die neuen Vorgaben der DS-GVO anzupassen. Eine Verarbeitung personenbezogener Daten ist nach dem 25.05.2018 nur noch rechtmäßig, wenn sie entsprechend der DS-GVO erfolgt. Einen Bestandsschutz für Alt-Sachverhalte oder eine weitere Übergangsfrist gibt es nicht.

Anwendung der DS-GVO

Die DS-GVO ist – vereinfacht gesagt - anzuwenden, wenn personenbezogene Daten automatisiert verarbeitet werden. Ein personenbezogenes Datum liegt immer dann vor, wenn sich eine Information auf eine zumindest identifizierbare natürliche Person bezieht. Eine Verarbeitung erfasst jeden Vorgang im Zusammenhang mit personenbezogenen Daten. Umfasst sind also viele Prozesse, angefangen von der Kundendatenbank eines Unternehmens bis hin zur Lohnbuchhaltung. Es kommt dabei nicht einmal darauf an, ob das Unternehmen allein im B2B-Bereich tätig ist, da schon der Name einer Kontaktperson ein personenbezogenes Datum darstellt.

Zwar ist der Datenschutz in Deutschland nicht neu, allerdings wird er mit der DS-GVO auf eine neue Grundlage gestellt. Der Unternehmer wird als für die Datenverarbeitung Verantwortlicher in das Zentrum des Datenschutzes gestellt. Er muss dafür Sorge tragen, dass alle Datenverarbeitungsprozesse im Unternehmen datenschutzkonform ablaufen und hat diese Überwachung zu dokumentieren. Dabei ist unter der DS-GVO bereits die Nicht-Dokumentation ein sanktionierbarer Verstoß. Neben der Einführung neuer und umfassender Dokumentationspflichten und der Anwendungserweiterungen für Unternehmen außerhalb der EU werden insbesondere die Bußgeldsanktionen ausgeweitet. Mit allen drei Aspekten reagiert der europäische Gesetzgeber darauf, dass der Datenschutz bisher keine ausreichende Beachtung

fand.

Neue und höhere Bußgelder

Für Verstöße gegen die einzelnen Bestimmungen der DS-GVO können nun Bußgelder von bis zu 20 Mio. Euro oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden, je nachdem, welcher der Beträge höher ist. Bei „kleineren“ Verstößen – welche die DS-GVO explizit als solche nennt – sind 10 Mio. Euro oder 2% des Umsatzes möglich. Im Vergleich zum vorher geltenden BDSG-alt ist der Bußgeldrahmen damit um etwa das Sechzigfache erhöht worden. Allein dieser Faktor macht deutlich, dass Bußgelder im Zeitalter der DS-GVO höher ausfallen müssen.

Viel entscheidender in der Praxis ist aber zunächst, in welchen Fällen ein Bußgeld droht. Durch die DS-GVO werden bestimmte Pflichten für das Unternehmen in Deutschland neu eingeführt. Eine ist bspw. die Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO oder die Pflicht, Vorkehrungen zur Erfüllung der Rechte der Betroffenen nach Artt. 12 ff. DS-GVO zu treffen. Daneben sind bereits nach altem Recht vorhandene Pflichten nun erstmalig bußgeldbewehrt. Das gilt beispielsweise für die Pflicht zum Führen eines Verzeichnisses von Verarbeitungstätigkeiten oder die Pflicht Maßnahmen zur Datensicherheit zu treffen.

Verzeichnis von Verarbeitungstätigkeiten

Der erste Schritt zur Vermeidung eines Bußgelds ist daher das Aufstellen eines Verzeichnisses von Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO. Das Instrument eines Verfahrensverzeichnisses ist in Deutschland nicht neu, es war auch bisher nach den Regelungen des (alten) Bundesdatenschutzgesetzes (BDSG) für Verfahren der automatisierten Verarbeitung personenbezogener Daten ein Verzeichnis zu führen (§§ 4d ff. BDSG). Allerdings konnte auch kein Bußgeld verhängt werden, wenn ein solches Verzeichnis nicht geführt wurde. Das führte dazu, dass das Thema in der Praxis sehr stiefmütterlich behandelt wurde.

Im Verfahrensverzeichnis für Verantwortliche nach Art. 30 Abs. 1 DS-GVO sind der Name des verantwortlichen Unternehmens mitsamt Kontaktdaten aufzuführen. Daneben ist festzuhalten, ob noch ein weiteres Unternehmen an der Verarbeitung beteiligt ist (sog. „gemeinsam mit ihm Verantwortlicher“). Ebenso sind Name und Kontaktdaten des Datenschutzbeauftragten zu nennen, sofern einer benannt worden ist.

Für jede Verarbeitungstätigkeit sind die Zwecke zu beschreiben (bspw. Personalverwaltung, Werbung, Cloud-Services) und zusätzlich die Kategorien der betroffenen Personen (Beispiel: Mitarbeiter, Kunden) sowie die Kategorien der personenbezogenen Daten (Beispiel: Nutzungsdaten, Kontaktdaten)

Weiter sind die Kategorien von Empfängern zu beschreiben, gegenüber denen die personenbezogenen Daten offengelegt werden. Empfänger können alle natürlichen, juristischen Personen, Behörden oder unternehmensinterne Stellen sein, die Daten planmäßig erhalten sollen. Zu den Empfängern zählt insbesondere der Auftragsverarbeiter.

Wenn personenbezogene Daten an ein Drittland oder eine internationale Organisation übermittelt werden, so sind diese ebenfalls in dem Verfahrensverzeichnis namentlich zu dokumentieren mitsamt den Garantien, warum die Datenübermittlung ausnahmsweise zulässig ist.

Der Verantwortliche hat in dem Verzeichnis möglichst konkret darzulegen, welche Regelungen er getroffen hat zur Löschung der Daten. Daten sind unverzüglich zu löschen, wenn der Zweck der Verarbeitung erfüllt ist und keine gesetzlichen Aufbewahrungspflichten bestehen.

Letztlich muss jedes Verarbeitungsverzeichnis eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DS-GVO enthalten. Hier reicht in der Regel ein

Verweis auf das allgemeine Sicherheitskonzept, sodass nur davon abweichende oder zusätzliche Maßnahmen aufzuzählen sind, welche die konkret beschriebene Verarbeitung betreffen.

Das Verfahrensverzeichnis kann darüber hinaus durch weitere Informationen ergänzt werden. Dies kann sinnvoll sein, um im Zweifelsfall die Rechtmäßigkeit der Verarbeitung vollständig nachweisen zu können. Weitere Informationen können etwa Angaben zur Rechtsgrundlage der Verarbeitungen sein (Art. 5 Abs. 1 DS-GVO) oder das Ergebnis einer Datenschutz-Folgeabschätzung (Art. 35 DS-GVO).

Verzeichnis von Verarbeitungstätigkeiten des Auftragsverarbeiters

Neu – und nicht schon im BDSG-alt vorhanden – ist ab dem 25.05.2018 die Pflicht für Auftragsverarbeiter zur Führung eines speziellen eigenen Verfahrensverzeichnisses. Der Inhalt ist in Art. 30 Abs. 2 DS-GVO geregelt. Es unterscheidet sich vom Verzeichnis für den Verantwortlichen nach Art. 30 Abs. 1 DS-GVO vor allem in seinem Umfang.

Unterschiede beim Verfahrensverzeichnis des Auftragsverarbeiters

Das Verzeichnis des Verantwortlichen und das des Auftragsverarbeiters unterscheiden sich vor allem in Ihrem Detailgrad. Während der Verantwortliche den Zweck der Verarbeitung sowie die Kategorien der Daten und Empfänger angeben muss, sind es beim Auftragsverarbeiter (nur) die Kategorien der auftragsgemäß durchgeführten Verarbeitungstätigkeiten. Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) nennt als Beispiele für Verarbeitungskategorien u.a. Finanzbuchhaltung, Lohn- und Gehaltsabrechnungen, Personalverwaltung oder die Werbeadressenverarbeitung in einem Letter-Shop.

Zu beachten ist, dass der Auftragsverarbeiter für Verarbeitungen in seiner Zuständigkeit (bspw. die eigene Personalverwaltung) **zusätzlich** ein Verfahrensverzeichnis für Verantwortliche nach Art. 30 Abs. 1 DS-GVO zu führen hat.

Ausnahmen für das Führen eines Verzeichnisses

Grundsätzlich hat jeder Verantwortliche und jeder Auftragsverarbeiter ein Verzeichnis von Verarbeitungstätigkeiten anzulegen und laufend zu aktualisieren. Eine Ausnahme von dieser grundsätzlichen Pflicht besteht für Unternehmen, die weniger als 250 Mitarbeiter beschäftigen. Diese Ausnahme gilt allerdings nicht, wenn die Verarbeitung personenbezogener Daten ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung nicht nur gelegentlich erfolgt oder eine

Verarbeitung besonderer in der DS-GVO beschriebener Datenkategorien erfolgt, wie etwa Gesundheitsdaten.

Informationspflichten

Darüber hinaus sind gegebenenfalls die unternehmensinternen Prozesse umzustellen. So sind beispielsweise Personen ab dem 25.05.2018 zu informieren, wenn personenbezogene Daten von ihnen erhoben werden. In dieser Information ist auch die Rechtsgrundlage zu nennen, auf welche die Datenerhebung gestützt wird. Daneben ist unter anderem zu nennen, wie lange die Daten gespeichert werden. Diese in Art. 13 DS-GVO geregelten Informationspflichten sind weitgehend neu, sodass Unternehmer ihre Informationen entsprechend anpassen müssen. Vor allem vor dem Hintergrund, dass auch ein Verstoß gegen die Informationspflicht bußgeldbewehrt ist.

Pflicht zur Benennung eines Datenschutzbeauftragten

Privatwirtschaftliche Unternehmen benennen einen Datenschutzbeauftragten in jedem Fall, wenn die Kerntätigkeit des Verantwortlichen eine umfangreiche systematische Überwachung Betroffener erforderlich macht, oder wenn die Kerntätigkeit in der umfangreichen Verarbeitung sensibler personenbezogener Daten besteht (Art. 9 oder Art. 10 DS-GVO). Zusätzlich müssen Unternehmen einen Datenschutzbeauftragten benennen, wenn sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen (§ 38 Abs. 1 BDSG-neu). Die nationale Ausgestaltung führt somit dazu, dass ein Großteil der deutschen Unternehmen die Pflicht hat einen Datenschutzbeauftragten zu benennen. Ein Verstoß gegen die Benennungspflicht ist ebenfalls bußgeldbewehrt mit einem sog. „kleinen“ Bußgeld von bis zu 10 Mio. Euro oder 2% des weltweiten Jahresumsatzes.

Bußgeldhöhe

Ein Vergleich zu Bußgeldern, die nach altem Recht verhängt wurden, verbietet sich bereits aufgrund der Neuausrichtung des Datenschutzes durch die DS-GVO. Denn Bußgelder sollen europaweit einheitlich verhängt werden, sodass schon deshalb die vorherige nationale Praxis nicht herangezogen werden kann.

Daneben gibt die DS-GVO vor, dass ein Bußgeld „in jedem Einzelfall wirksam, verhältnismäßig und abschreckend“ sein muss. Der Grundsatz der Verhältnismäßigkeit führt zwar dazu, dass die Umstände des Einzelfalls berücksichtigt werden müssen. Man sollte sich gleichwohl nicht darauf verlassen, dass ein Bußgeld nicht auch ruinös sein kann.

Ausblick

Gerade die vorangegangene Praxis der deutschen Aufsichtsbehörden mit Augenmaß und Bedacht zu sanktionieren, lässt hoffen, dass Bußgelder ein letztes Mittel sind und die Beratung der Aufsichtsbehörden im Vordergrund steht. Denn wenn der Datenschutz im Unternehmen nicht ignoriert wird sowie im Großen und Ganzen die wesentlichen Pflichten erfüllt werden, haben die Aufsichtsbehörden auch den Spielraum an ihrer bisherigen Praxis festzuhalten und zunächst kein Bußgeld zu verhängen. Das kann jedoch nicht gelten, wenn die Pflichten der DS-GVO auch nicht ansatzweise erfüllt werden. Es hängt deshalb wesentlich von den Unternehmen ab. Keine Aufsichtsbehörde wird den Spielraum haben, bei einer drastischen oder vollständigen Ignoranz kein Bußgeld zu verhängen. Eine „Gnadenfrist“ über den 25.05.2018 hinaus wird nicht gewährt. Dies haben die zuständigen Aufsichtsbehörden bereits deutlich zum Ausdruck gebracht. Das bedeutet eben auch, dass ab dem genannten Stichtag nicht nur Sanktionen durch die Aufsichtsbehörden drohen, sondern insbesondere wettbewerbsrechtliche Abmahnungen von Verbänden sowie von Konkurrenten.

Autor

Nils Steffen
Rechtsanwalt
Datenschutzbeauftragter (TÜV)

Derra, Meyer & Partner Rechtsanwälte PartGmbB
Frauenstr. 14
89073 Ulm
Tel.: +49 731 92 288 0

Soweit für heute. Schön, dass Sie hier angekommen sind. Wir würden uns sehr über Rückmeldungen und Kommentare zum Beitrag freuen. Wenn Ihnen unser Blog gefällt, wäre es schön, wenn Sie den Beitrag an einen oder mehrere Kollegen schicken oder in den sozialen Medien teilen würden. Nutzen Sie die entsprechenden Funktionen am Ende der Seite.

PS. Schon auf unserer Facebook-Seite vorbei geschaut?
http://www.facebook.com/Unternehmensberatung.mareco
Fan werden und nichts mehr verpassen!

| Kommentieren |

0 Kommentar/e