Sonderinformation zum Datenschutz

Datenschutz wird verschärft – neue Datenschutz – Grundverordnung ab dem 25. Mai 2018

Sehr geehrte Mandantin,
sehr geehrter Mandant,

wie wir Ihnen bereits in der aktuellen Mandanten-Information 01-2018 angekündigt haben, informieren wir Sie nun hinsichtlich der „Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG“ (EU-DSGVO).

Die „Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG“ (EU-DSGVO) gilt ab dem 25. Mai 2018. Für alle Mitgliedstaaten in der Europäischen Union regelt sie verbindlich die Vorschriften zur Verarbeitung von personenbezogenen Daten. Die Rechte der betroffenen Personen werden zu neuen Strukturen in den Datenschutzsystemen führen müssen, damit die Bußgeld- und Strafvorschriften keine erhöhten Gefahren für die Unternehmen darstellen. Mit Schreiben v. 12.1.2018 - IV A 3 - S 0030/16/10004-07 [CAAAG-69827] hat das BMF bereits die AEAO (Anwendungserlass zur AO) entsprechend der EU-DSGVO angepasst.

I. Geltungsbereich

Die bisherige Datenschutzregelung (Richtlinie 95/46/EG) und das bisherige Bundesdatenschutzgesetz werden ab dem 25. Mai 2018 ersetzt. Eine Umsetzung in nationales Recht ist nicht notwendig, denn die EU-DSGVO gilt als unmittelbare Verordnung in jedem Mitgliedstaat.
Gewisse Gestaltungsmöglichkeiten werden jedoch durch die Einfügung von Öffnungsklauseln und Spezialklauseln ermöglicht. Diese hat der deutsche Gesetzgeber durch das Bundesdatenschutzgesetz 2018 bereits entsprechend genutzt. Das Bundesdatenschutzgesetz wird ebenfalls am 25. Mai 2018 in Kraft treten.

Büro Dresden:
Comeniusstraße 32
01307 Dresden
E-mail: info@wp-heide.com
Web: www.wp-heide.com
Telefon: 0049 (0) 351 44 00 38 0
Telefax: 0049 (0) 351 44 00 38 29

Büro Freiberg:
Erbische Straße 18
09599 Freiberg
Telefon: 0049 (0) 3731 77 31 77
Telefax: 0049 (0) 3731 77 31 78

Praxishinweis

Es ist nur noch ein kurzer Zeitraum, bis die neuen Rechte der betroffenen Personen gelten. Bereits im Vorfeld müssen Schwachstellen des Datenschutzes ermittelt und das System angepasst werden. Die Systemanpassung ist je nach Unternehmenszweig und Umfang von gespeicherten personenbezogenen Daten umständlich und kann große Personalressourcen kosten. Sorgen Sie vor und ermitteln Sie den Bedarf, denn geeignetes Personal im Bereich Datenschutz ist auf dem Markt kostbar geworden.

II. Anwendungsbereich

Die Verordnung regelt mit ihren Vorschriften den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und den freien Verkehr dieser Daten. Dabei sollen die Grundrechte und die Grundfreiheiten natürlicher Personen geschützt werden.

Was sind personenbezogene Daten?

Personenbezogene Daten sind gemäß Art. 4 Nr. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder einem oder mehreren besonderen Merkmalen identifiziert werden kann. Diese sind Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Personen. Oder verkürzt: Personenbezogen sind **alle Daten, die eine Identifizierung einer Person ermöglichen**.
Die DSGVO gilt für ganz oder teilweise automatisiert erfolgende Verarbeitungen von personenbezogenen Daten. Bei nicht automatisierten Verarbeitungen gilt die DSGVO nur dann, wenn die personenbezogenen Daten in einem Dateisystem erfasst werden oder erfasst werden sollen. Damit ist jede Erfassung in ein Computersystem oder durch entsprechende Programme von der DSGVO betroffen.

Praxishinweis

Grundsätzlich sind alle diese Daten betroffen, die in irgendeiner Weise mithilfe von Computern oder Computerprogrammen gespeichert werden.
Die Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, wenn

- diese im Rahmen der Tätigkeiten einer Niederlassung in der Union erfolgt oder
- keine Niederlassung in der Union besteht und die Datenverarbeitung den betroffenen Personen in der Union Waren oder Dienstleistungen anbietet. Damit sind auch Unternehmen wie beispielsweise Facebook, Amazon oder Google von der Datenschutzgrundverordnung betroffen und müssen diese beachten (vgl. Art. 3 Abs. 2 DSGVO).

Praxishinweis

Voraussichtlich werden insbesondere kleine und mittlere Unternehmen mit der Umsetzung der Verordnung zu kämpfen haben. Die großen o. g. Unternehmen können durch ihre eigenen bereits bestehenden Datenschutzabteilungen Anpassungen aufgrund eines bestehenden Personalstamms vornehmen, während kleinere Unternehmen teilweise erstmalig eigene Abteilungen zur Sicherstellung der Verordnung und zur Vermeidung von Bußgeldern aufbauen werden. Dass es lediglich einen Mitarbeiter in einer Datenschutzabteilung in einem Unternehmen gibt, wird vermutlich bald der Vergangenheit angehören.

III. Verantwortlicher und Auftragsverarbeiter

Der Verantwortliche ist gemäß Art. 24 DSGVO der Verarbeiter der Daten. Er muss alle Maßnahmen treffen, die zur Erfüllung der Verarbeitung der Daten notwendig sind. Zur Sicherstellung und Nachweiserbringung, dass die Bearbeitung ordnungsgemäß erfolgt, setzt er geeignete technische und organisatorische Maßnahmen um. Hierbei berücksichtigt er die Art, den Umfang, die Umstände und den Zweck der Verarbeitung sowie die Risiken, die für die Rechte und Freiheiten natürlicher Personen drohen.

Was sind geeignete technische und organisatorische Maßnahmen?

Was geeignet ist, hängt alleine davon ab, in welchem Umfang personenbezogene Daten gespeichert werden. Dies ist von Unternehmen zu Unternehmen unterschiedlich und kann nicht einheitlich festgestellt werden. Im Grunde sollten die Rechte des Betroffenen gewährleistet werden. Wenn dies möglich ist, sollten die Maßnahmen zum Datenschutz geeignet sein, um der Verordnung zu entsprechen.

Diese Maßnahmen zum Datenschutz müssen erforderlichenfalls überprüft und entsprechend der aktuellen Situation angepasst werden. Damit wird ein **Compliance-System ausschließlich für die Verarbeitung der personenbezogenen Daten** verlangt. Dieses muss Nachprüfungen bezüglich der Einhaltung der Vorschriften und Aktualisierungen an die tatsächlichen Gegebenheiten zulassen. Nur auf diese Weise kann sichergestellt werden, dass die Verordnung tatsächlich eingehalten wird und somit die Rechte der Betroffenen gewährleistet werden.

IV. Grundsätze der Datenerfassung

Die personenbezogenen Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.
Die Daten sind gemäß Art. 5 Abs. 1 Buchst. e DSGVO zweckgebunden zu erfassen, d. h. sie sind für festgelegte, eindeutige und legitime Zwecke zu erheben und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Die Zweckbindung soll die unbegrenzte Sammlung von Daten begrenzen und nachvollziehbar machen, welchem Zweck die Datenerfassung und Vorhaltung dient. Entsprechend dem Zweck müssen die Daten in einem angemessenen Rahmen und für den Zweck erheblichen Umfang verarbeitet werden. Diese Verarbeitung soll auf ein **notwendiges Maß** beschränkt sein (vgl. Datenminimierung, Art. 5 Abs. 1 Buchst. c DSGVO).

<u>Praxishinweis</u>

Werden große Mengen an Daten gesammelt, sollte der Zweck für jeden Datenbestandteil einzeln ermittelt und bestimmt werden können. Es bleibt nämlich abzuwarten, welche „Genauigkeit“ bei der Zweckbestimmung verlangt werden wird. Insbesondere Mandanten, die gezielt personalisierte Werbung mit den personenbezogenen Daten betreiben, werden sich Gedanken über die Definition des Zwecks machen müssen. Ansonsten könnte ihnen Maßlosigkeit vorgeworfen werden.
Die personenbezogenen Daten müssen nach Art. 5 Abs. 1 Buchst. d DSGVO sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Unrichtige Daten sind unverzüglich zu löschen.

Praxishinweis

Fraglich wird sein, wie die Aktualität sichergestellt werden kann. Eine Möglichkeit wäre, dass Sie in bestimmten Zeitabständen eine Befragung der Betroffenen durchführen oder bei der Einwilligung darauf hinweisen, dass Änderungen der maßgeblichen personenbezogenen Daten mitzuteilen sind. Außerdem sollte im Unternehmen sichergestellt werden, dass Mitarbeiter Mitteilungen über Änderungen durch den Betroffenen auch tatsächlich verarbeiten.

Die personenbezogenen Daten sind nur so lange zu speichern, wie die Identifizierung der betroffenen Personen für die Zwecke, für die sie verarbeitet werden, erforderlich ist (vgl. Speicherbegrenzung, Art. 5 Abs. 1 Buchst. e DSGVO).

Praxishinweis

Es müssen Zeitrahmen bestimmt werden, für die die gespeicherten Daten vorzuhalten sind, und Zeitpunkte benannt werden, ab denen bestimmte oder alle Daten rückstandslos zu löschen sind. Diese Zeitrahmen und Zeitpunkte werden je nach Mandant und Unternehmenstätigkeit variieren. Neben der Wahrung der Integrität und der Vertraulichkeit muss auch die **Sicherheit der personenbezogenen Daten** gewährleistet werden. Das bedeutet, dass der unbefugte Zugriff, die unbefugte Verarbeitung, die unbeabsichtigte Zerstörung oder unbeabsichtigte Schädigung der Daten oder der Verlust durch technische und organisatorische Maßnahmen sicherzustellen sind (vgl. Art. 5 Abs. 1 Buchst. f DSGVO).

Hinweis

Neu und beachtlich ist die Regelung der Rechenschaftspflicht in Art. 5 Abs. 2 DSGVO. Das bedeutet: Die vorbezeichneten Grundsätze sind nicht nur durch die Unternehmen einzuhalten, sondern die Einhaltung der Grundsätze muss auch nachgewiesen werden. Damit wird eine Datenschutzdokumentation notwendig, die den Grundsätzen entspricht und im Rahmen eines Compliance-Systems überwacht werden muss.

V. Rechtmäßigkeit der Verarbeitung und Bedingungen für die Einwilligung

Mit der Rechtsmäßigkeit der Verarbeitung wird bestimmt, wann und welche personenbezogenen Daten gespeichert werden dürfen. Es existieren mehrere mögliche Bedingungen, die eine **Speicherung von personenbezogenen Daten zulassen**:

- Die betroffene Person hat ihre Einwilligung zur Verarbeitung für einen oder mehrere bestimmte Zwecke gegeben.
- Die Verarbeitung der Daten erfolgt für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist.
- Stellt die betroffene Person eine vertragliche Anfrage, ist eine Speicherung auch für vorvertragliche Maßnahmen erlaubt, wenn dies erforderlich ist.
- Besteht die Notwendigkeit der Datenverarbeitung für die Erfüllung einer Verpflichtung oder für lebenswichtige Interessen, ist auch eine solche Verarbeitung rechtmäßig.

Die Einwilligung muss vom Verarbeiter der Daten nachgewiesen werden. Eine schriftliche Erklärung hierzu ist in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu verfassen (vgl. Art. 7 Abs. 1 und 2 DSGVO). Die Einwilligung kann jedoch gemäß Art. 7 Abs. 3 DSGVO jederzeit widerrufen werden. Die bis zum Widerruf verarbeiteten Daten werden dadurch nicht rechtswidrig, wovon die betroffene Person zum Zeitpunkt der Einwilligung in Kenntnis gesetzt werden muss.

VI. Rechte der betroffenen Personen

Werden personenbezogene Daten gespeichert, so hat der Verantwortliche nach Art. 13 Abs. 1 DSGVO der betroffenen Person zum Zeitpunkt der Erhebung eine Mitteilung über die zu verarbeitenden Daten zu geben. Er muss Folgendes mitteilen:

- Namen und die Kontaktdaten des Verantwortlichen (ggf. des Datenschutzbeauftragten),
- Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung,
- ggf. berechtigte Interessen des Verantwortlichen oder eines Dritten,
- Empfänger der personenbezogenen Daten.

Neben den vorbezeichneten Informationen sind zum Zeitpunkt der Erhebung der Daten u. a. anzugeben, wie lange die Daten gespeichert werden oder Kriterien zu bestimmen, die eine Festlegung der Dauer gewährleisten. Des Weiteren muss über die Rechte aufgeklärt werden, und zwar über das Recht

- der Auskunft,
- der Berichtigung,
- der Löschung,
- der Einschränkung der Verarbeitung,
- des Widerspruchs gegen die Verarbeitung sowie
- auf Datenübertragbarkeit.

Auf das Recht, einen Widerspruch gegen eine Verarbeitung einzulegen, soll in einer klaren, einfachen und adressatengerechten Sprache ausdrücklich hingewiesen werden. Außerdem soll ein solcher Widerspruch kostenfrei möglich sein.
Wird durch den Verantwortlichen angestrebt, die Daten zu einem anderen Zweck zu verarbeiten als den, für den die personenbezogenen Daten erhoben wurden, so muss er für eine solche Weiterverarbeitung Informationen über diesen anderen Zweck zur Verfügung stellen (vgl. Art. 13 Abs. 2 und 3 DSGVO).

Hinweis:

Eine wesentliche Neuerung ist gemäß Art. 17 DSGVO das „**Recht auf Vergessenwerden“.** Demnach kann eine betroffene Person von einem Verantwortlichen die Löschung der personenbezogenen Daten verlangen, wenn die Daten

- für den vorgesehenen Zweck nicht mehr notwendig sind oder
- die betreffende Person ihre Einwilligung widerrufen oder das Widerspruchsrecht ausgeübt hat.

Außerdem muss eine Löschung vorgenommen werden, wenn die Löschung gesetzlich vorgeschrieben ist oder die personenbezogenen Daten unrechtmäßig verarbeitet wurden. Die Rechteinhaber behalten somit die Kontrolle über ihre Daten und können insbesondere durch den Widerruf und den Löschungsantrag auf den Umgang und die Speicherung ihrer Daten einwirken.

VII. Bei Verstoß drohen Geldbußen und Strafen

Der Datenschutz erfolgt gemäß Art. 1 DSGVO zu Wahrung der Grundrechte und der Grundfreiheiten natürlicher Personen. Damit wird der Verstoß gegen die ordnungsgemäße Verarbeitung von personenbezogenen Daten nicht mehr einfach hingenommen. Stattdessen wird in Art. 83 DSGVO festgelegt, dass ein Verstoß zu einer Geldbuße führt, die in jedem Einzelfall wirksam, verhältnismäßig, aber auch abschreckend wirken soll.

Bei der Verhängung einer Geldbuße ist u. a. Folgendes zu berücksichtigen:
- die Art, die Schwere und die Dauer eines Verstoßes sowie
- der Umfang, der Zweck und die Zahl der Betroffenen der Datenverarbeitung sowie
- der erlittene Schaden.

Zu unterscheiden ist auch, ob Vorsatz oder Fahrlässigkeit vorliegt. Darüber hinaus muss berücksichtigt werden, ob eine Schadenswiedergutmachung stattgefunden hat und ob bereits früher Verstöße begangen worden sind. Schließlich ist auch der Grund der Verantwortung des Verantwortlichen und die Kategorie der betroffenen Daten bei der Berechnung der Geldbuße von Relevanz.

Die Geldbuße kann bis zu 20 Mio. € betragen oder im Falle eines Unternehmens bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres. Gemäß Art. 83 Abs. 6 DSGVO wird der jeweils höhere Betrag als Geldbuße festgesetzt.

Praxishinweis

Das stiefmütterliche Betreiben einer Datenschutzabteilung im Unternehmen dürfte mit den drohenden Geldbußen ein Ende haben, denn der Schaden des Unternehmens bei einem nicht funktionierenden System kann immens sein. Deshalb sollte von Anfang an ein klares Konzept mit klaren Dokumentationen zur Gewährleistung der Rechte der betroffenen Personen und zur Umsetzung der Verordnung vorhanden sein. Neben den Geldbußen sollten außerdem die Strafvorschriften einen Grund darstellen, dass die Verordnung ernst genommen und umgesetzt wird.

Gemäß Art. 43 DSGVO werden Strafvorschriften durch das jeweilige Mitgliedsland selber bestimmt. Der Bundesgesetzgeber hat dies mit der Vorschrift § 42 BDSG n. F. getan:
- Nach dieser Vorschrift wird mit Freiheitsstrafe **bis zu drei Jahren oder Geldstrafe** bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen – ohne hierzu berechtigt zu sein – einem Dritten übermittelt oder auf andere Art und Weise zugänglich macht und hierbei gewerbsmäßig handelt.
- Mit Freiheitsstrafe **bis zu zwei Jahren oder Geldstrafe** wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind – ohne hierzu berechtigt zu sein – verarbeitet oder durch unrichtige Angaben erschleicht und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

Es handelt sich um ein Antragsdelikt, so dass gemäß § 42 Abs. 3 BDSG n. F. die Tat nur auf Antrag verfolgt wird. Antragsberechtigt sind die betroffene Person, der Verantwortliche, die oder der Beauftragte und die Aufsichtsbehörde.

Fazit

Der Datenschutz wird verschärft, und die Rechte der betroffenen Personen werden erheblich erweitert. Damit die Verordnung auch umgesetzt wird, hat der Gesetzgeber neue Bußgeld- und Strafvorschriften erlassen. Insbesondere die Höhe der drohenden Bußgelder ist durch die Bemessung am Jahresumsatz des Vorjahres für große Unternehmen mit einem großen Risiko behaftet. Durch die notwendige Einwilligung zur Speicherung personenbezogener Daten kann eigenverantwortlich bestimmt werden, in welchem Umfang diese gespeichert werden. Das Auskunftsrecht gewährleistet anschließend, dass eine Kontrolle über die gespeicherten Daten durch betroffene Personen möglich ist. Aufgrund dieser Kontrolle können die Rechte auf Löschung, Berichtigung oder Beschränkung wirksam geltend gemacht werden. Das „Recht auf Vergessenwerden“ stellt den ersten Vorstoß gegen die Tatsache dar, dass in der digitalen Welt Daten grundsätzlich nicht mehr einfach vollständig gelöscht werden können. Es wird sich zeigen, wie insbesondere die internetbasierten Firmen dieses Recht umsetzen. Abschließend ist festzustellen, dass die EU-Datenschutzgrundverordnung die Unternehmen vor große Herausforderungen stellen wird, da die Datenschutzkonzepte überarbeitet und neu strukturiert werden müssen. Es wird jedoch keine Lösung für alle geben. Insofern sind entsprechend der Speicherung personenbezogener Daten individuelle Lösungen für das jeweilige Unternehmen oder für die jeweilige Branche notwendig.

Büro Dresden:
Comeniusstraße 32
01307 Dresden
E-mail: info@wp-heide.com
Web: www.wp-heide.com
Telefon: 0049 (0) 351 44 00 38 0
Telefax: 0049 (0) 351 44 00 38 29

Büro Freiberg:
Erbische Straße 18
09599 Freiberg
Telefon: 0049 (0) 3731 77 31 77
Telefax: 0049 (0) 3731 77 31 78