

Erläuterungen und Text der einschlägigen, gesetzlichen Vorschriften

Dieses Merkblatt gibt Ihnen die Möglichkeit, das Wichtigste noch einmal nachzulesen. Sollten Sie Fragen haben, insbesondere wenn es darum geht, ob ein bestimmter Umgang mit personenbezogenen Daten erlaubt ist, zögern Sie nicht, Ihren Vorgesetzten oder unseren Datenschutzbeauftragten, Herrn Mirko Tasch (Tel: +49 8142 42050 10, Email: datenschutz@fristo.de) zu fragen.

Was schützt das Datenschutzrecht?

Ihre Vertraulichkeitsverpflichtung dient – wie das gesamte Datenschutzrecht – dem Schutz des Persönlichkeitsrechts derjenigen Menschen, um deren Daten es sich handelt. Diese Menschen nennt das Gesetz „betroffene Personen“. Das können unsere Kunden sein, Ihre Kollegen – oder auch Sie als unser Mitarbeiter.

Das Persönlichkeitsrecht gibt jedem Menschen das Recht, grundsätzlich selbst darüber zu entscheiden, wer was über ihn wissen darf. Beispielsweise darf jeder Kunde selbst entscheiden, wer seinen Wohnort erfahren soll, und Sie dürfen entscheiden, wer Ihren Gesundheitszustand kennen darf. Es ist Ihre Entscheidung, ob das geheim bleibt oder Sie es veröffentlichen.

Ausnahmen, in denen nicht nur der Wille des Betroffenen gilt, muss es natürlich geben – aber jede Ausnahme braucht nach dem Gesetz eine Rechtfertigung. Das kann nach der Regelung eine Einwilligung der betroffenen Person oder eine gesetzliche Erlaubnis sein. Die wichtigste gesetzliche Erlaubnis gilt für diejenigen Daten, die unbedingt benötigt werden, um einen Vertrag mit der betroffenen Person zu erfüllen. Deshalb darf Ihr Vermieter beispielsweise Ihren Namen speichern, ohne dass Sie einwilligen müssten.

Was sind meine Pflichten?

Sie müssen personenbezogene Daten nicht nur vertraulich behandeln, Sie dürfen sie zum Beispiel nicht an Dritte weitergeben oder offen herumliegen lassen. Das Gesetz verpflichtet Sie vielmehr dazu, nur dann mit personenbezogenen Daten zu arbeiten, wenn dies erlaubt ist – unabhängig davon, ob Sie diese Daten beispielsweise lesen, notieren, löschen oder weitergeben. Diese Erlaubnis müssen einerseits wir als Unternehmen haben, andererseits aber auch Sie persönlich nach unserer unternehmensinternen Aufgabenverteilung. Die gesetzlichen Vertraulichkeitspflichten einzuhalten, ist also auch Ihre ganz persönliche Verpflichtung.

Bitte beachten Sie: Ihre Vertraulichkeitsverpflichtung gilt zeitlich unbefristet, und zwar selbst dann, wenn Sie nicht mehr für uns tätig sind. Sie gilt gegenüber allen Personen, die nicht dienstlich für die jeweilige Sache zuständig sind – also auch gegenüber allen anderen Kollegen, Ihrer Familie und der Presse.

Wenn Sie mit personenbezogenen Daten arbeiten, müssen Sie sich dabei immer an die Weisungen Ihres Vorgesetzten halten. Sollte im Fall von Auftragsverarbeitung Ihr Vorgesetzter Ihnen eine bestimmte Weisung erteilen, unser Kunde aber eine andere Weisung, geht die Weisung unseres Kunden vor, solange unser Kunde nichts Verbotenes verlangt.

In ganz besonderen Fällen kann auch ein Gesetz vorschreiben, personenbezogene Daten z. B. an eine Behörde herauszugeben. Widersprüchliche Weisungen und gesetzliche Verarbeitungspflichten sind sehr selten, und die damit verbundenen komplizierten Rechtsfragen werden Sie kaum alleine entscheiden können. Wenden Sie sich daher bitte immer sofort an Ihren Vorgesetzten oder den betrieblichen Datenschutzbeauftragten falls einer bestellt wurde.

Was sind personenbezogenen Daten?

Das Datenschutzrecht gilt für alle „personenbezogenen Daten“. Personenbezogene Daten sind Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person, also einen Menschen, beziehen (Art. 4 Nr. 1 DS-GVO). Das kann die Angabe sein, dass jemand Mitglied in einem Verein ist, wo er wohnt oder wie viel Geld er auf dem Konto hat.

Personenbezogenes Datum kann aber auch die Angabe sein, dass die Kontonummer 123456 ihren Dispokredit überzogen hat. Denn obwohl hier kein Name genannt wird, ist einfach zu ermitteln, wer Inhaber dieses Kontos ist: Es handelt sich um Angaben zu einer „identifizierbaren“ Person. Eine Person ist identifizierbar, wenn man – eigene und fremde – Informationen kombinieren kann und dadurch erfährt, um wen es sich handelt. Das geht sehr viel einfacher als man denkt: So konnten Forscher jeden einzelnen von 1,5 Millionen Menschen eindeutig identifizieren, wenn sie nur wussten, wo er sich zu elf beliebigen Zeitpunkten aufhielt (<https://www.taz.de/!5070185/>). Auch genügen Geburtsdatum, Postleitzahl und Geschlecht, um 87 Prozent der US-Amerikaner eindeutig zu identifizieren (http://www.chip.de/artikel/Re-Identifizierung-Die-neue-Kunst-der-Datenkraken-3_46575146.html).

Auch wenn Sie selbst denken, dass bestimmte Daten niemandem zuzuordnen sind, dürfen Sie diese deshalb nicht ohne Zustimmung Ihres Vorgesetzten und des betrieblichen Datenschutzbeauftragten an Dritte weitergeben oder veröffentlichen – abgesehen davon, dass es sich auch um Betriebsgeheimnisse handeln könnte, die Sie ebenfalls streng vertraulich behandeln müssen.

Unsere Pflichten als Unternehmen

Wir als Unternehmen und Sie als unser Mitarbeiter dürfen personenbezogene Daten nur dann verarbeiten, wenn es dafür eine Rechtsgrundlage gibt. Art. 4 Nr. 2 DS-GVO beschreibt den Begriff der Verarbeitung äußerst weit, so dass er letztlich jeden Kontakt mit personenbezogenen Daten umfasst: „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“. Als mögliche Rechtsgrundlage nennt Art. 6 Abs. 1 DS-GVO eine Einwilligung der betroffenen Person und verschiedene gesetzliche Erlaubnisse.

Für welche Daten es bei welchem Verfahren eine solche Rechtsgrundlage gibt, sagt Ihnen Ihr Vorgesetzter. Bitte beachten Sie: Andere Daten dürfen Sie nicht verwenden. Personenbezogene Daten dürfen zudem nur zu dem jeweils bestimmt festgelegten Zweck verwendet werden. Eine Zweckänderung braucht eine eigene Rechtsgrundlage.

Das bedeutet, dass z. B. Kundendaten, die bisher nur für die Vertragsabwicklung verwendet wurden, nicht ohne Weiteres für Werbung genutzt werden dürfen. Auch hier sagt Ihnen Ihr Vorgesetzter, ob eine Zweckänderung erlaubt ist.

Als wichtigste Regel sollten Sie sich hier merken, dass Sie personenbezogene Daten nie aus eigener Entscheidung heraus weitergeben oder für sich selbst nutzen (beispielsweise außerhalb dienstlicher Notwendigkeit lesen) dürfen.

Außerdem müssen personenbezogene Daten geschützt werden, so dass Unbefugte keine Kenntnis von ihnen nehmen und dass sie auch nicht versehentlich verloren gehen können. Deshalb verschlüsseln wir personenbezogene Daten, wenn wir sie über das Internet übertragen müssen, und machen regelmäßig Sicherungskopien (Backups). Das Gesetz verpflichtet uns zu vielen weiteren Sicherheitsmaßnahmen. So dürfen z. B. Ausdrucke mit personenbezogenen Daten oder Datenträger wie CDs, USB-Sticks oder Festplatten keinesfalls einfach weggeworfen oder weggegeben werden, sondern müssen ordnungsgemäß geschreddert oder durch die EDV-Abteilung sicher gelöscht werden.

Dass Sie Ihr Passwort nicht an Kollegen oder Dritte weitergeben oder gar auf einem Zettel an den Computer kleben dürfen, sollte sich von selbst verstehen – es ist Ihr persönliches Passwort, und wenn es jemand missbraucht, sind Sie persönlich dafür verantwortlich (siehe „Folgen von Verstößen“).

Welche Rechte haben betroffenen Personen?

Einer der wichtigsten Aspekte des Persönlichkeitsrechts ist es, zu wissen, was andere über einen wissen. Wenn ein Unternehmen Daten über jemanden sammelt, muss es daher fast immer die betroffene Person informieren. Jeder Mensch kann zudem von jedem Unternehmen eine Kopie der Daten verlangen, die das Unternehmen über ihn gespeichert hat (Art. 15 DS-GVO). Dies bedeutet, dass alles, was Sie beispielsweise über einen Kunden notieren, auch schriftlich zu diesem Kunden gelangen kann. Achten Sie deshalb bitte darauf, dass Sie nur Angaben notieren, für die wir auch eine Erlaubnis zum Speichern haben – Ihr Vorgesetzter sagt Ihnen, welche Daten das in Ihrem konkreten Fall sind. Und achten Sie bitte auch darauf, wie Sie es aufschreiben: knapp, neutral und niemals beleidigend o. ä. Das Auskunftsrecht ist ein spezielles Recht des Betroffenen: An andere Personen und Stellen dürfen wir normalerweise keine Auskünfte geben – das wäre eine Übermittlung, für die wir eine Erlaubnis bräuchten.

Benötigen wir bestimmte Daten nicht mehr, müssen wir sie löschen (Art. 17 DS-GVO); falsche Daten müssen wir berichtigen (Art. 16 DS-GVO). Wenn Sie feststellen, dass nicht mehr benötigte Daten weiterhin gespeichert bleiben, sprechen Sie bitte Ihren Vorgesetzten darauf an. Denn die Speicherung von Daten, die eigentlich zu löschen wären, kann mit Geldbußen bis 20.000.000 EUR oder vier Prozent des weltweiten Jahresumsatzes des gesamten Konzerns – je nachdem, was höher ist – bestraft werden. Zusätzlich haben betroffene Personen einen Anspruch auf Schadensersatz einschließlich Schmerzensgeld für die Verletzung ihres Rechts auf Datenschutz.

Jede betroffene Person kann uns zudem verbieten, ihre Daten für Werbezwecke zu benutzen (Art. 21 Abs. 2, 3 und 5 DS-GVO) und hat auch in bestimmten anderen Fällen ein Widerspruchsrecht (Art. 21 Abs. 1 DS-GVO). Betroffene Personen haben zudem weitere Rechte, die aber für Sie als Mitarbeiter normalerweise nicht von Bedeutung sind.

Sollte ein Auskunftersuchen, ein Widerspruch oder ein anderer Wunsch oder Hinweis mit Datenschutzbezug bei Ihnen eingehen, leiten Sie ihn bitte sofort an [den betrieblichen Datenschutzbeauftragten] weiter. Selbstständig dürfen Sie solche Dinge nur bearbeiten, wenn wir Ihnen diese Aufgabe ausdrücklich zugewiesen haben. In Zweifelsfällen fragen Sie den betrieblichen Datenschutzbeauftragten (Telefon [...]). Beachten Sie bitte, dass auch Behörden oder die Polizei nicht ohne Weiteres Daten von uns erhalten können. Wir benötigen hier einen förmlichen Beschlagnahmebeschluss. In bestimmten Fällen genügt ein förmliches Auskunftersuchen. Wenn Sie von der Polizei oder einer anderen Behörde kontaktiert werden, informieren Sie bitte sofort Ihren Vorgesetzten und den betrieblichen Datenschutzbeauftragten.

Folgen von Verstößen

Verstöße gegen das Datenschutzrecht können für [Unternehmen] schwerwiegende Folgen haben – aber auch für Sie persönlich.

Fast alle Verstöße gegen das Datenschutzrecht können mit Geldbuße bestraft werden (Art. 83 DS-GVO). Diese Geldbuße kann bis zu 20.000.000 EUR pro Verstoß betragen oder für uns als Unternehmen bis zu vier Prozent des weltweiten Jahresumsatzes des gesamten Konzerns, je nachdem, was höher ist. Geldbußen können sogar gegen einzelne Mitarbeiter verhängt werden: Geben Sie beispielsweise ohne eine entsprechende Anweisung von [Unternehmen] personenbezogene Daten weiter oder nutzen Sie sie für Ihre eigenen Zwecke, können Sie persönlich mit einer Geldbuße bis zu 20.000.000 EUR bestraft werden. Zudem sind bestimmte Verstöße gegen das Datenschutzrecht Straftaten, die mit Gefängnis bestraft werden können (§ 42 BDSG): Beispiel: Jemand verkauft weisungswidrig eine Festplatte mit personenbezogenen Daten anstatt sie zu zerstören.

Verstöße gegen das Datenschutzrecht können zudem nach anderen Gesetzen strafbar sein, z. B. nach § 17 UWG (Verrat von Geschäfts- und Betriebsgeheimnissen), § 202 a StGB (Ausspähen von Daten) oder § 263 a StGB (Computerbetrug).

Jede betroffene Person kann Schadensersatz für eine unzulässige Verarbeitung ihrer Daten verlangen, und zwar einschließlich Schmerzensgeld für die Persönlichkeitsrechtsverletzung (Art. 82 DS-GVO, §§ 823 ff. BGB). Unter Umständen müssen Sie persönlich diesen Schadensersatz ganz oder teilweise bezahlen, wenn Sie mittlere oder schwere Verstöße begangen oder personenbezogene Daten weisungswidrig verarbeitet haben, etwa für Ihre eigenen Zwecke genutzt haben. Fragen Sie daher lieber einmal zu viel als zu wenig.

Schwere Schäden für [Unternehmen] kann es verursachen, wenn eine so genannte Datenpanne öffentlich bekannt wird. Kunden verlieren das Vertrauen und kaufen nicht mehr bei uns, wenn sie nicht sicher sein können, dass ihre Daten bei uns in guten Händen sind. Hinzu kommt, dass wir nach Art. 34 Abs. 1 und Abs. 3 lit. c DS-GVO verpflichtet sein können, eine Datenpanne allen Betroffenen mitzuteilen oder gar öffentlich bekanntzumachen. Bitte helfen Sie mit, dass es niemals dazu kommt.

Nicht zuletzt können wir arbeitsrechtliche Konsequenzen ziehen, wenn Sie gegen Ihre Vertraulichkeitspflichten verstoßen. Denkbar sind je nach Schwere Ihres Fehlverhaltens insbesondere eine Abmahnung, eine fristgerechte Kündigung oder sogar eine fristlose Kündigung ohne vorherige Verwarnung.

Neue Verfahren mit personenbezogenen Daten

Sie sind an einem Projekt beteiligt, bei dem personenbezogene Daten eine Rolle spielen? Dann sorgen Sie bitte dafür, dass der betriebliche Datenschutzbeauftragte von Anfang an einbezogen wird. Er kann Ihnen sagen, ob es überhaupt rechtlich möglich ist, was Ihr Projektteam plant, und Tipps geben, was Sie verbessern könnten, insbesondere, welche Anforderungen wir zu „Privacy by Design“ und „Privacy by Default“ (Art. 25 DS-GVO) oder zur

Sicherheit (Art. 32 DS-GVO) einhalten müssen. Wenn Sie diese Fragen rechtzeitig mit dem betrieblichen Datenschutzbeauftragten klären, können Sie von Anfang an das richtige Verfahren entwickeln. Wenn Sie ihn erst kurz vor Schluss einbeziehen, kann es sein, dass Ihr Projekt komplett scheitert, weil es rechtlich nicht oder nur unter aufwendigen Änderungen umzusetzen ist. [Optional: Außerdem sind Sie nach Art. 38 Abs. 1 DS-GVO verpflichtet, den betrieblichen Datenschutzbeauftragten ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen einzubinden, unter Umständen eine Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO durchzuführen und das Verfahren zum Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DS-GVO anzumelden. Werden Dritte eingeschaltet, etwa weil wir den Server nicht selbst betreiben, müssen besondere Verträge abgeschlossen werden (Art. 28 DS-GVO).] Wichtig ist, dass wir als Unternehmen jederzeit beweisen können, dass wir das Gesetz vollständig einhalten (Art. 5 und 24 DS-GVO). Können wir diesen Nachweis nicht vollständig erbringen, haften wir auf Schadensersatz und Geldbußen – und auch Sie persönlich, wenn Sie das Verfahren ohne Genehmigung eingeführt haben.

Besondere Hinweise für Nutzer von Internet und E-Mail

Internet und E-Mail sind sehr praktisch, weil man innerhalb von Sekunden Daten ans andere Ende der Welt schicken kann. Gerade diese Geschwindigkeit macht sie aber auch so risikoreich. Hinzu kommt, dass das Internet als Medium zur Kommunikation zwischen Wissenschaftlern erfunden wurde, die sich gegenseitig absolut vertrauen konnten. Deshalb gibt es standardmäßig keine Sicherheitsmaßnahmen. Das ist heute nicht mehr angemessen und eine große Gefahr für vertrauliche Daten. Denn eine E-Mail ist eigentlich nichts anderes als eine elektronische Postkarte, die vom Wind durch die Stadt getrieben und immer wieder von allen möglichen Leuten aufgehoben, angeschaut und wieder in die Luft geworfen wird. Deshalb beachten Sie bitte folgende Grundregeln:

Vertrauliche Daten – insbesondere auch personenbezogene Daten – dürfen Sie niemals per normaler E-Mail versenden. Wenn die EDV-Abteilung Ihren Computer mit einem Programm zur E-Mail-Verschlüsselung ausgestattet hat und der Empfänger der E-Mail ebenfalls solch ein Programm verwendet, können Sie ihm eine verschlüsselte Nachricht schicken, die gegen Abhören und Manipulation geschützt ist. [Optional: Für bestimmte Empfänger hat die EDV-Abteilung eine automatische Verschlüsselung eingerichtet. Hierzu erhalten Sie eine gesonderte schriftliche Nachricht.] Bitte prüfen Sie aber in jedem Fall vorher, ob Sie die Daten überhaupt an den Empfänger weitergeben dürfen!

Bevor Sie eine E-Mail versenden, achten Sie bitte unbedingt darauf, ob der richtige Empfänger im Adressfeld steht. Hier liegt eine große Fehlerquelle, wenn mehrere Leute einen ähnlichen Namen oder eine ähnliche E-Mail-Adresse haben. Schauen Sie vor dem Abschicken noch einmal genau darauf! Durch solche Verwechslungen sind schon extrem vertrauliche Informationen an die Öffentlichkeit gekommen.

Beachten Sie den Unterschied zwischen „To:/An:“ (Empfänger), „CC:“ (Kopie) und „BCC:“ (Blindkopie): Jeder Empfänger der E-Mail sieht sämtliche anderen Empfänger, die im To:- bzw. CC:-Feld stehen. Soll ein Empfänger für die anderen nicht sichtbar sein, müssen Sie ihn ins BCC:-Feld schreiben. Die Daten aller To:-/CC:-Empfänger übermitteln Sie im rechtlichen Sinne an die anderen Empfänger. Und dafür benötigen Sie, wie Sie wissen, eine Erlaubnis. Wenn Sie Nachrichten an viele Empfänger senden müssen, sprechen Sie deshalb bitte mit der EDV-Abteilung, ob dafür eine Mailing-Liste o. ä. eingerichtet werden sollte, oder ob die Versendung über das BCC:-Feld ausreichend ist. Es wurden bereits Bußgelder gegen Mitarbeiter verhängt, die alle Empfänger ins To:-Feld geschrieben haben!

Sie dürfen niemals vertrauliche Daten an Ihren privaten E-Mail-Account weiterleiten oder woanders als auf unseren Servern speichern – insbesondere nicht in der „Cloud“. Dies bedeutet unter anderem, dass Sie auch keinesfalls eine automatische Weiterleitung Ihres E-Mail-Accounts an Ihre private E-Mail-Adresse einrichten dürfen.

Vertrauen Sie nicht zu sehr auf E-Mails. Absenderangaben von E-Mails lassen sich problemlos fälschen – vertrauen können Sie nur digital signierten und verschlüsselten E-Mails, falls Sie ein entsprechendes Programm von der EDV-Abteilung erhalten haben. Seien Sie daher bitte auch sehr vorsichtig, wenn Sie unaufgefordert E-Mails mit Anhängen (Attachments) oder Links erhalten: Oftmals enthalten diese Anhänge Schadprogramme (Viren). Wir versuchen, Viren so gut wie möglich auszufiltern, dass sie überhaupt nicht in Ihrem Postfach ankommen – aber die Kriminellen sind uns häufig ein Stück voraus. Bevor Sie einen solchen Anhang öffnen, fragen Sie bitte im Zweifel bei der Geschäftsleitung bzw. der EDV-Abteilung nach.

Beachten Sie bitte außerdem unsere interne Richtlinie.

Gesetzestexte:

Artikel 29 DSGVO - Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters

Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.

Artikel 83 DSGVO Allgemeine Bedingungen für die Verhängung von Geldbußen

(1) Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

(2) Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich zu oder anstelle von Maßnahmen nach Artikel 58 Absatz 2 Buchstaben a bis h und i verhängt. 2Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag wird in jedem Einzelfall Folgendes gebührend berücksichtigt:

- a) 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;
- b) Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;
- c) jegliche von dem Verantwortlichen oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens;
- d) Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß den Artikeln 25 und 32 getroffenen technischen und organisatorischen Maßnahmen;
- e) etwaige einschlägige frühere Verstöße des Verantwortlichen oder des Auftragsverarbeiters;
- f) Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelpen und seine möglichen nachteiligen Auswirkungen zu mindern;
- g) Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind;
- h) 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;
- i) Einhaltung der nach Artikel 58 Absatz 2 früher gegen den für den betreffenden Verantwortlichen oder Auftragsverarbeiter in Bezug auf denselben Gegenstand angeordneten Maßnahmen, wenn solche Maßnahmen angeordnet wurden;

j) Einhaltung von genehmigten Verhaltensregeln nach Artikel 40 oder genehmigten Zertifizierungsverfahren nach Artikel 42 und

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

(3) Verstößt ein Verantwortlicher oder ein Auftragsverarbeiter bei gleichen oder miteinander verbundenen Verarbeitungsvorgängen vorsätzlich oder fahrlässig gegen mehrere Bestimmungen dieser Verordnung, so übersteigt der Gesamtbetrag der Geldbuße nicht den Betrag für den schwerwiegendsten Verstoß.

(4) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

a) die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43;

b) die Pflichten der Zertifizierungsstelle gemäß den Artikeln 42 und 43;

c) die Pflichten der Überwachungsstelle gemäß Artikel 41 Absatz 4.

(5) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

a) die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6, 7 und 9;

b) die Rechte der betroffenen Person gemäß den Artikeln 12 bis 22;

c) die Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation gemäß den Artikeln 44 bis 49;

d) alle Pflichten gemäß den Rechtsvorschriften der Mitgliedstaaten, die im Rahmen des Kapitels IX erlassen wurden;

e) Nichtbefolgung einer Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Artikel 58 Absatz 2 oder Nichtgewährung des Zugangs unter Verstoß gegen Artikel 58 Absatz 1.

(6) Bei Nichtbefolgung einer Anweisung der Aufsichtsbehörde gemäß Artikel 58 Absatz 2 werden im Einklang mit Absatz 2 des vorliegenden Artikels Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist.

(7) Unbeschadet der Abhilfebefugnisse der Aufsichtsbehörden gemäß Artikel 58 Absatz 2 kann jeder Mitgliedstaat Vorschriften dafür festlegen, ob und in welchem Umfang gegen Behörden und öffentliche Stellen, die in dem betreffenden Mitgliedstaat niedergelassen sind, Geldbußen verhängt werden können.

(8) Die Ausübung der eigenen Befugnisse durch eine Aufsichtsbehörde gemäß diesem Artikel muss angemessenen Verfahrensgarantien gemäß dem Unionsrecht und dem Recht der Mitgliedstaaten, einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren, unterliegen.

(9) 1 Sieht die Rechtsordnung eines Mitgliedstaats keine Geldbußen vor, kann dieser Artikel so angewandt werden, dass die Geldbuße von der zuständigen Aufsichtsbehörde in die Wege geleitet und von den zuständigen nationalen Gerichten verhängt wird, wobei sicherzustellen ist, dass diese Rechtsbehelfe wirksam sind und die gleiche Wirkung wie die von Aufsichtsbehörden verhängten Geldbußen haben. 2 In jeden Fall müssen die verhängten Geldbußen wirksam, verhältnismäßig und abschreckend sein. 3 Die betreffenden Mitgliedstaaten teilen der Kommission bis zum 25. Mai 2018 die Rechtsvorschriften mit, die sie aufgrund dieses Absatzes erlassen, sowie unverzüglich alle späteren Änderungsgesetze oder Änderungen dieser Vorschriften.

§ 42 BDSG neu - Strafvorschriften

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein,

1. einem Dritten übermittelt oder
2. auf andere Art und Weise zugänglich macht

und hierbei gewerbsmäßig handelt.

(2) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind,

1. ohne hierzu berechtigt zu sein, verarbeitet oder
2. durch unrichtige Angaben erschleicht

und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

(3) 1 Die Tat wird nur auf Antrag verfolgt. 2 Antragsberechtigt sind die betroffene Person, der Verantwortliche, die oder der Bundesbeauftragte und die Aufsichtsbehörde.

(4) Eine Meldung nach Artikel 33 der Verordnung (EU) 2016/679 oder eine Benachrichtigung nach Artikel 34 Absatz 1 der Verordnung (EU) 2016/679 darf in einem Strafverfahren gegen den Meldepflichtigen oder Benachrichtigenden oder seine in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden.

§ 43 BDSG neu - Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 30 Absatz 1 ein Auskunftsverlangen nicht richtig behandelt oder
2. entgegen § 30 Absatz 2 Satz 1 einen Verbraucher nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.

(3) Gegen Behörden und sonstige öffentliche Stellen im Sinne des § 2 Absatz 1 werden keine Geldbußen verhängt.

(4) Eine Meldung nach Artikel 33 der Verordnung (EU) 2016/679 oder eine Benachrichtigung nach Artikel 34 Absatz 1 der Verordnung (EU) 2016/679 darf in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen den Meldepflichtigen oder Benachrichtigenden oder seine in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden.