Verpflichtung zum Datengeheimnis

Ich wurde heute darüber belehrt, dass personenbezogene Daten, also alle Informationen, die sich auf einen benannten oder identifizierbaren Menschen beziehen, nicht unbefugt erhoben, genutzt, weitergegeben oder sonst verarbeitet werden dürfen.

Ich verpflichte mich, personenbezogene Daten vertraulich zu behandeln und ausschließlich auf Weisung von zu verarbeiten. Diese Vertraulichkeitsverpflichtung besteht auch nach Beendigung meiner Tätigkeit für fort.

Mir ist bekannt, dass Verstöße gegen meine Vertraulichkeitsverpflichtung nach Art. 83 der Datenschutz-Grundverordnung (DSGVO), §§ 42 und 43 des Bundesdatenschutzgesetzes (BDSG) und anderen Gesetzen mit Geldbußen bis zu 20.000.000 EUR, Geld- oder Freiheitsstrafe geahndet werden können. Eine Verletzung meiner Vertraulichkeitsverpflichtung kann zugleich eine Verletzung arbeitsvertraglicher Pflichten oder spezieller Geheimhaltungspflichten darstellen und beispielsweise zu Abmahnung, fristloser oder fristgerechter Kündigung und/oder Schadensersatzpflichten führen.

Gesetzliche Folge von Verstößen gegen meine Vertraulichkeitsverpflichtung können auch Schadensersatzansprüche der Personen, auf die die Daten sich beziehen, gegen mich persönlich sein, für die ich unter Umständen unbeschränkt mit meinem gesamten Vermögen und ohne Möglichkeit einer Restschuldbefreiung in einem Insolvenzverfahren hafte. Sonstige Geheimhaltungsverpflichtungen, etwa aus dem Arbeitsvertrag, bestehen neben dieser Vertraulichkeitsverpflichtung.

[Ort, Datum, Unterschrift der belehrenden Person]

Ich bestätige, dass ich heute über die Bedeutung meiner Verpflichtung zur Verschwiegenheit über personenbezogene Daten belehrt wurde. Ein Exemplar dieses Formulars sowie ein Merkblatt mit Erläuterungen und dem Text der Art. 29 DSGVO, Art. 83 Abs. 4–6 DSGVO, § 42 Abs. 1 und 2 BDSG und § 43 Abs. 1 und 2 BDSG habe ich erhalten.

[Ort, Datum, Unterschrift des Mitarbeiters]

Merkblatt zur Vertraulichkeitsverpflichtung

Sie werden heute über Ihre Pflichten im Umgang mit personenbezogenen Daten unterrichtet und unterzeichnen eine entsprechende Vertraulichkeitsverpflichtung. 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 den betrieblichen Datenschutzbeauftragten (Telefon oder E-Mail) zu fragen.

Datenschutz schützt das Persönlichkeitsrecht

Ihre Vertraulichkeitsverpflichtung dient – wie das gesamte Datenschutzrecht – dem Schutz des Persönlichkeitsrechts derjenigen Menschen, auf die sich die Daten beziehen. Diese Menschen nennt das Gesetz „betroffene Personen". Das können unsere Kunden sein, Ihre Kollegen – oder auch Sie als unsere Mitarbeiterin oder unser Mitarbeiter.

Das Persönlichkeitsrecht gibt jedem Menschen das Recht, grundsätzlich selbst darüber zu entscheiden, wer was über ihn wissen darf.

Ausnahmen, in denen nicht nur der Wille des Betroffenen gilt, bedürfen einer gesetzlichen Rechtfertigung. Das kann eine Einwilligung der betroffenen Person oder eine gesetzliche Erlaubnis sein (z.B. für diejenigen Daten, die unbedingt benötigt werden, um einen Vertrag mit der betroffenen Person zu erfüllen).

Neben der DSGVO, die in der gesamten Europäischen Union gilt, gibt es in Deutschland un-ter anderem auch noch das BDSG, das bestimmte Sonderfälle regelt, insbesondere den Beschäftigtendatenschutz.

Der Begriff „personenbezogene Daten"

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

Eine Person ist identifizierbar, wenn man – eigene und fremde – Informationen kombinieren kann und dadurch erfährt, um wen es sich handelt.

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.

Für welche Daten das Datenschutzrecht gilt

Das Datenschutzrecht gilt einerseits für Daten, welche mittels eines Computers verarbeitet werden (wozu auch die Daten vieler technischer Geräte zählen), aber auch für „die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen" (Art. 2 Abs. 1 DSGVO). Unter Dateisystem ist jede geordnete Ablage zu verstehen (Art. 4 Nr. 6 DSGVO) – etwa eine alphabetische Sammlung aus-gefüllter Formulare. Das Datenschutzrecht gilt zudem auch dann, wenn die Daten später in einer Datei gespeichert werden sollen oder aus einer Datei stammen – etwa eine ausgedruckte Liste mit Kundendaten.

Daten von Mitarbeiterinnen und Mitarbeitern oder Bewerberinnen und Bewerbern werden in jeder Form durch das BDSG geschützt, auch wenn es sich um einen unsortierten Stapel handschriftlicher Notizen handelt, der weggeworfen werden soll.

Ihre Vertraulichkeitspflichten

Sie müssen personenbezogene Daten nicht nur vertraulich behandeln, Sie dürfen sie z.B. 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.

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 Kolleginnen und Kollegen, Ihrer Familie und der Presse.

Wenn Sie mit personenbezogenen Daten arbeiten, müssen Sie sich dabei immer an die Weisungen Ihres Vorgesetzten halten. In ganz besonderen Fällen kann auch ein Gesetz vorschreiben, personenbezogene Daten z.B. an eine Behörde herauszugeben.

Unsere und Ihre Pflichten

Wir als Unternehmen und Sie als unser Mitarbeiter dürfen personenbezogene Daten nur dann verarbeiten, wenn es dafür eine Rechtsgrundlage gibt. Art. 4 Nr. 2 DSGVO beschreibt den Begriff der Verarbeitung äußerst weit, sodass er letztlich jeden Kontakt mit personenbezogenen Daten umfasst.

Für welche Daten es bei welchem Verfahren eine solche Rechtsgrundlage gibt, sagt Ihnen Ihr Vorgesetzter oder der Datenschutzbeauftragte. 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 oder der Datenschutzbeauftragte, 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 gelten bei uns bestimmte technische und organisatorische Maßnahmen. So dürfen zB. Ausdrucke mit personenbezogenen Daten oder Datenträger wie CDs, USB-Sticks oder Fesplatten keinesfalls einfach weggeworfen oder weggegeben werden, sondern müssen ordnungsgemäß geschreddert oder durch die EDV-Abteilung sicher gelöscht werden.

Auch dürfen Sie Ihr Passwort niemals an Kollegen oder Dritte weitergeben oder gar auf einem Zettel an den Computer heften. Es ist Ihr persönliches Passwort, und wenn es jemand missbraucht, sind Sie persönlich dafür verantwortlich (siehe „Folgen von Verstößen“).

Rechte der betroffenen Personen

Wenn ein Unternehmen Daten über jemanden sammelt, muss es 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 DSGVO). 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 oder der Datenschutzbeauftragte sagen Ihnen, welche Daten das in Ihrem konkreten Fall sind.

Benötigen wir bestimmte Daten nicht mehr, müssen wir sie löschen (Art. 17 DSGVO); falsche Daten müssen wir berichtigen (Art. 16 DSGVO). Wenn Sie feststellen, dass nicht mehr benötigte Daten weiterhin gespeichert bleiben, sprechen Sie bitte Ihren Vorgesetzten oder den Datenschutzbeauftragten darauf an.

Jede betroffene Person kann uns zudem verbieten, ihre Daten für Werbezwecke zu benutzen (Art. 21 Abs. 2, 3 und 5 DSGVO) und hat auch in bestimmten anderen Fällen ein Widerspruchsrecht (Art. 21 Abs. 1 DSGVO).

Sollte ein Auskunftsersuchen, ein Widerspruch oder ein anderer Wunsch oder Hinweis mit Datenschutzbezug bei Ihnen eingehen, informieren Sie bitte umgehend den Datenschutzbeauftragen und Ihren Vorgesetzten. Selbstständig dürfen Sie solche Dinge nur bearbeiten, wenn wir Ihnen diese Aufgabe ausdrücklich zugewiesen haben. In Zweifelsfällen fragen Sie den betrieblichen Datenschutzbeauftragten. Beachten Sie bitte, dass auch Behörden oder die Polizei nicht ohne Weiteres Daten von uns erhalten können. 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 unser Unternehmen schwerwiegende Folgen haben – aber auch für Sie persönlich.

Fast alle Verstöße gegen das Datenschutzrecht können mit Geldbuße bestraft werden (Art. 83 DSGVO). 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 des Unternehmens 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 § 23 GeschGehG (Verletzung von Geschäftsgeheimnissen), § 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 DSGVO, §§ 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.

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.

Wichtige Vorschriften

Art. 4 DSGVO - Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

1. „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene 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 zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;

2. „Verarbeitung“ 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 andereForm der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

Art. 5 DSGVO Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen:

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffe-ne Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse lie-g ende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archiv-zwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

Art. 6 DSGVO – Rechtmäßigkeit der Verarbeitung

(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;

d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;

e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

(…)

Art. 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 die-se Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.

Art. 32 DSGVO – Sicherheit der Verarbeitung

(…)

(2) Bei der Bearbeitung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind – insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust oder Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

Art. 33 DSGVO – Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

(1) Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der […] zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.
(…)

Art. 82 Abs. 1 DSGVO – Haftung und Recht auf Schadenersatz

(1) Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadensersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

Art. 83 DSGVO – Allgemeine Bedingungen für die Verhängungen von Geld-bußen

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

(…)

(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.

§ 42 BDSG – 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.

(…)

§ 43 BDSG – Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 30 Abs. 1 ein Auskunftsverlangen nicht richtig behandelt oder

2. entgegen § 30 Abs. 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 T**TDSG – Vertraulichkeit der Kommunikation – Fernmeldegeheimnis**

(1) Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

(2) Zur Wahrung des Fernmeldegeheimnisses sind verpflichtet

1. Anbieter von öffentlich zugänglichen Telekommunikationsdiensten sowie natürliche und juristische Personen, die an der Erbringung solcher Dienste mitwirken,
2. Anbieter von ganz oder teilweise geschäftsmä0ig angebotenen Telekommunikationsdiensten sowie natürliche und juristische Personen, die an der Erbringung solcher Dienste mitwirken,
3. Betreiber öffentlicher Telekommunikationsnetze und
4. Betreiber von Telekommunikationsanlagen, mit denen geschäftsmäßig Telekommunikationsdienste erbracht werden.

Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.

(3) Den nach Absatz 2 Satz 1 Verpflichteten ist es untersagt, sich oder anderen über das für die Erbringung der Telekommunikationsdienste oder für den Betrieb ihrer Telekommunikationsnetze oder ihrer Telekommunikationsanlagen einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder von den näheren Umständen der Telekommunikation zu verschaffen. Sie dür-fen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen nur für den in Satz 1 genannten Zweck verwenden. Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit die-ses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei aus-drücklich auf Telekommunikationsvorgänge bezieht. Die Anzeigepflicht nach § 138 des Strafgesetzbuches hat Vorrang.

(4) Befindet sich die Telekommunikationsanlage an Bord eines Wasser- oder Luftfahrzeugs, so besteht die Pflicht zur Wahrung des Fernmeldegeheimnisses nicht gegenüber der Person, die das Fahrzeug führt, und ihrer Stellvertretung.

§ 206 StGB – Verletzung des Post- oder Fernmeldegeheimnisses

(1) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigtem eines Unternehmens bekanntgeworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer als Inhaber oder Beschäftigter eines in Absatz 1 bezeichneten Unternehmens unbefugt

1. eine Sendung, die einem solchen Unternehmen zur Übermittlung anvertraut worden und verschlossen ist, öffnet oder sich von ihrem Inhalt ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft,
2. eine einem solchen Unternehmen zur Übermittlung anvertraute Sendung unterdrückt oder
3. eine der in Absatz 1 oder in Nummer 1 oder 2 bezeichneten Handlungen gestattet oder fördert.

(3) Die Absätze 1 und 2 gelten auch für Personen, die

1. Aufgaben der Aufsicht über ein in Absatz 1 bezeichnetes Unternehmen wahrnehmen,
2. von einem solchen Unternehmen oder mit dessen Ermächtigung mit dem Erbringen von Post- oder Telekommunikationsdiensten betraut sind oder
3. mit der Herstellung einer dem Betrieb eines solchen Unternehmens dienenden Anlage oder mit Arbeiten daran betraut sind.

(4) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die ihm als außerhalb des Post- oder Telekommunikationsbereichs tätigem Amtsträger auf Grund eines befugten oder unbefugten Eingriffs in das Post- oder Fernmeldegeheimnis bekanntgeworden sind, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(5) Dem Postgeheimnis unterliegen die näheren Umstände des Postverkehrs bestimmter Personen sowie der Inhalt von Postsendungen. Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

§ 23 GeschGehG – Verletzung von Geschäftsgeheimnissen

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer zur Förderung des eigenen oder fremden Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber eines Unternehmens Schaden zuzufügen,

1. entgegen § 4 Absatz 1 Nummer 1 ein Geschäftsgeheimnis erlangt,
2. entgegen § 4 Absatz 2 Nummer 1 Buchstabe a ein Geschäftsgeheimnis nutzt oder offenlegt oder
3. entgegen § 4 Absatz 2 Nummer 3 als eine bei einem Unternehmen beschäftigte Person ein Geschäftsgeheimnis, da ihr im Rahmen des Beschäftigungsverhältnisses anvertraut worden oder zugänglich gemacht worden ist, während der Geltungsdauer des Beschäftigungsverhältnisses offenlegt.

(2) Ebenso wird bestraft, wer zur Förderung des eigenen oder fremden Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber eines Unternehmens Schaden zuzufügen, ein Geschäftsgeheimnis nutzt oder offenlegt, das er durch eine fremde Handlung nach Absatz 1 Nummer 2 oder Nummer 3 erlangt hat.

(3) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer zur För-derung des eigenen oder fremden Wettbewerbs oder aus Eigennutz entgegen § 4 Absatz 2 Nummer 2 oder Nummer 3 ein Geschäftsgeheimnis, das eine ihm im geschäftlichen Verkehr anvertraute geheime Vorlage oder Vorschrift technischer Art ist, nutzt oder offenlegt.

(4) Mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe wird bestraft, wer

1. in den Fällen des Absatzes 1 oder des Absatzes 2 gewerbsmäßig handelt,
2. in den Fällen des Absatzes 1 Nummer 2 oder Nummer 3 oder des Absatzes 2 bei der Offenlegung weiß, dass das Geschäftsgeheimnis im Ausland genutzt werden soll, oder
3. in den Fällen des Absatzes 1 Nummer 2 oder des Absatzes 2 das Geschäftsgeheimnis im Ausland nutzt.

(5) Der Versuch ist strafbar.

(6) Beihilfehandlungen einer in § 53 Absatz 1 Satz 1 Nummer 5 der Strafprozessordnung genannten Person sind nicht rechtswidrig, wenn sie sich auf die Entgegennahme, Auswertung oder Veröffentlichung des Geschäftsgeheimnisses beschränken.

(7) § 5 Nummer 7 des Strafgesetzbuches gilt entsprechend. Die §§ 30 und 31 des Strafgesetzbuches gelten entsprechend, wenn der Täter zur Förderung des eigenen oder fremden Wettbewerbs oder aus Eigennutz handelt.

(8) Die Tat wird nur auf Antrag verfolgt, es sei denn, dass die Strafverfolgungsbehörden wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.