

Merkblatt zur Wahrung gesetzlicher Bestimmungen zur Geheimhaltung

Verpflichtungserklärung auf Waren der Vertraulichkeit und Beachtung des Datenschutzes, Wahrung von Geschäftsgeheimnissen und des Fernmeldegeheimnisses

1. Wahrung der Vertraulichkeit und Beachtung des Datenschutzes

Da Sie im Rahmen Ihrer Tätigkeit möglicherweise mit personenbezogenen Daten in Kontakt kommen, verpflichte ich Sie hiermit zur Beachtung des Datenschutzes, insbesondere zur Wahrung der Vertraulichkeit. Ihre Verpflichtung besteht umfassend. Sie dürfen personenbezogene Daten selbst nicht ohne Befugnis verarbeiten und Sie dürfen anderen Personen diese Daten nicht unbefugt mitteilen oder zugänglich machen. Sie sind insbesondere verpflichtet, die datenschutzrechtlichen Vorgaben und Weisungen im Unternehmen zu beachten.

Unter einer Verarbeitung versteht die EU-Datenschutz-Grundverordnung (DSGVO) 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.

„Personenbezogene Daten“ im Sinne der DSGVO sind alle Informationen, die sich auf einen identifizierten oder identifizierbaren Menschen beziehen; als identifizierbar wird ein Mensch angesehen, der 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 identifiziert werden kann, die Ausdruck seiner physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.

Personenbezogene Daten dürfen daher nur verarbeitet werden, wenn eine Einwilligung bzw. eine gesetzliche Regelung die Verarbeitung erlauben oder eine Verarbeitung dieser Daten vorgeschrieben ist. Die Grundsätze der DSGVO für die Verarbeitung personenbezogener Daten sind in Art. 5 Abs. 1 DSGVO (siehe Merkblatt) festgelegt.

Unter Geltung des Art. 83 DSGVO können Verstöße gegen Datenschutzbestimmungen nach § 42 BDSG (Bundesdatenschutzgesetz) sowie nach anderen Strafvorschriften mit Freiheits- oder Geldstrafe geahndet werden. Datenschutzverstöße können zugleich eine Verletzung arbeits- oder dienstrechtlicher Pflichten bedeuten und entsprechende Konsequenzen haben.

Datenschutzverstöße sind ebenfalls mit möglicherweise sehr hohen Bußgeldern für das Unternehmen bedroht, die gegebenenfalls zu Ersatzansprüchen Ihnen gegenüber führen können.

Ihre Verpflichtung besteht ohne zeitliche Begrenzung und auch nach Beendigung Ihrer Tätigkeit fort.

2. Verpflichtung auf das Fernmeldegeheimnis §§ 3 TTDSG, 206 StGB

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.

Verstöße gegen das Fernmeldegeheimnis können nach § 206 StGB, ggf. auch nach anderen Gesetzen, mit Bußgeld, Geld- oder Freiheitsstrafe geahndet werden. Eine Verletzung des Fernmeldegeheimnisses kann zugleich eine Verletzung arbeitsvertraglicher Pflichten darstellen und beispielsweise zu Abmahnung, fristloser oder fristgerechter Kündigung und/oder Schadensersatzpflichten führen. Das Datengeheimnis und sonstige Geheimhaltungsverpflichtungen, etwa aus dem Arbeitsvertrag, bestehen neben dem Fernmeldegeheimnis.

Merkblatt zur Wahrung gesetzlicher Bestimmungen zur Geheimhaltung

2.1 Das Fernmelde- oder Telekommunikationsgeheimnis

Das Fernmeldegeheimnis schützt nicht nur Telefonate und Faxe, sondern auch moderne Kommunikationsformen wie E-Mail. Es wird daher auch Telekommunikationsgeheimnis genannt. Es handelt sich um ein Grundrecht (Art. 10 des Grundgesetzes – GG), das in § 3 TTDSG genauer geregelt ist.

Nicht nur wir als Unternehmen, sondern auch Sie persönlich müssen das Fernmeldegeheimnis einhalten. Diese Pflicht ergibt sich übrigens bereits aus dem Gesetz § 3 TTDSG). Ihre heutige förmliche Verpflichtung auf das Fernmeldegeheimnis dient nur dazu, Ihnen deutlich zu machen, wie wichtig diese Pflicht ist.

Bitte beachten Sie: Das Fernmeldegeheimnis gilt zeitlich unbefristet, und zwar auch dann, wenn Sie nicht mehr für uns tätig sind (§ 3 Abs. 2 Satz 2 TTDSG). Es gilt gegenüber allen Personen, die nicht dienstlich für die jeweilige Sache zuständig sind – also auch gegenüber allen anderen Kollegen, Ihrer Familie und der Presse.

2.2 Ihre Pflicht zur Wahrung des Fernmeldegeheimnisses

Informationen, die dem Fernmeldegeheimnis unterliegen, müssen Sie absolut vertraulich behandeln. Sie dürfen also beispielsweise nicht Einzelverbindungsnachweise oder Logfiles über Telekommunikationsverbindungen auswerten, E-Mail-Postfächer einsehen oder Ähnliches, wenn keine Ausnahme vorliegt. Eine Ausnahme ist nach § 3 Abs. 3 S. 3 TTDSG nur gegeben, wenn uns die Erbringung der Telekommunikationsdienste und der Schutz der Telekommunikationssysteme nur möglich ist, wenn wir von bestimmten dem Fernmeldegeheimnis unterliegenden Informationen Kenntnis haben.

Beachten Sie bitte, dass diese Erlaubnisse nur soweit bestehen, wie die Kenntnis, Speicherung oder Nutzung unbedingt für den jeweiligen Zweck erforderlich ist. Müssen Sie zur Behebung eines technischen Fehlers beispielsweise unbedingt in eine Mailbox schauen, dürfen Sie dies nur insoweit, wie es sich nicht vermeiden lässt: Genügt es etwa, den Header einer E-Mail auszuwerten, dürfen Sie den Nachrichtentext selbst nicht lesen. Natürlich dürfen Sie Dinge, die dem Fernmeldegeheimnis unterliegen, auch dann nicht weitersagen, wenn Sie zur Administration ausnahmsweise legal davon Kenntnis erlangt haben – auch nicht Ihrem Vorgesetzten. Einzige Ausnahme: Wenn Sie zufällig davon erfahren, dass eine schwere, in § 138 StGB genannte Straftat geplant wird.

Bei Zuwiderhandlungen gegen das Fernmeldegeheimnis, drohen Ihnen dafür unter Umständen bis zu fünf Jahre Haft. § 206 StGB stellt es (unter anderem) unter Strafe, Informationen weiterzugeben, die dem Fernmeldegeheimnis unterliegen. Ebenfalls ist es strafbar, anvertraute Sendungen (insbesondere E-Mails) unbefugt zu unterdrücken, etwa zu löschen oder über längere Zeit zurückzuhalten. Bestimmte Verstöße gegen das TTDSG können zudem ein Bußgeld zur Folge haben.

3. Verpflichtung auf Wahrung von Geschäftsgeheimnissen

Über Angelegenheiten des Unternehmens, die beispielsweise Einzelheiten des Unternehmens betreffen, sowie über Geschäftsvorgänge und Zahlen des internen Rechnungswesens und alle als Geschäftsgeheimnisse zu definierenden Vorgänge nach § 2 Nr. 1 GeschGehG, ist- auch nach Beendigung des Beschäftigungsverhältnisses- von Ihnen Verschwiegenheit zu wahren, sofern sie nicht öffentlich bekannt geworden sind. Hierunter fallen auch Vorgänge von Drittunternehmen, mit denen Sie dienstlich befasst sind. Alle dienstlichen Tätigkeiten betreffenden Aufzeichnungen, Abschriften, Geschäftsunterlagen, Ablichtungen, dienstlicher oder geschäftlicher Vorgänge, die Ihnen überlassen oder von Ihnen angefertigt werden, sind vor Einsichtnahme Unbefugter zu schützen. Von diesen Verpflichtungen haben Sie Kenntnis genommen. Sie sind sich bewusst, dass Sie sich bei Verletzungen strafbar machen können, insbesondere nach § 23 GeschGehG.

Merkblatt zur Wahrung gesetzlicher Bestimmungen zur Geheimhaltung

MERKBLATT - Abschrift der gesetzlichen Vorschriften

Abschrift der Datenschutzgrundverordnung (DSGVO), des Bundesdatenschutzgesetzes (BDSG) und weiterer Strafvorschriften aus dem Strafgesetzbuch

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 identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;
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 andere Form 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 betroffene 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 liegende 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 öffentlich liegende Archivzwecke 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“);
- (2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können.

rt. 32 DSGVO Sicherheit der Verarbeitung

(...)

Merkblatt zur Wahrung gesetzlicher Bestimmungen zur Geheimhaltung

- (4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

Art. 83 DSGVO Allgemeine Bedingungen für die Verhängung von Geldbußen

(...)

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

§ 43 BDSG – 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.

Merkblatt zur Wahrung gesetzlicher Bestimmungen zur Geheimhaltung

- (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 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden

§ 202a StGB - Ausspähen von Daten

- (1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.
- (2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

§ 202b StGB - Abfangen von Daten

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

§ 202c StGB Vorbereiten des Ausspähens und Abfangens von Daten

- (1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er
 1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder
 2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.
- (2) § 149 Abs. 2 und 3 g gilt entsprechend.

§ 202d StGB – Datenhehlerei

- (1) Wer Daten (§ 202a Absatz 2), die nicht allgemein zugänglich sind und die ein anderer durch eine rechtswidrige Tat erlangt hat, sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.
- (2) Die Strafe darf nicht schwerer sein als die für die Vortat angedrohte Strafe.
- (3) Absatz 1 gilt nicht für Handlungen, die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen. Dazu gehören insbesondere
 1. solche Handlungen von Amtsträgern oder deren Beauftragten, mit denen Daten ausschließlich der Verwertung in einem Besteuerungsverfahren, einem Strafverfahren oder einem Ordnungswidrigkeitenverfahren zugeführt werden sollen, sowie
 2. solche beruflichen Handlungen der in § 53 Absatz 1 Satz 1 Nummer 5 der Strafprozessordnung genannten Personen, mit denen Daten entgegengenommen, ausgewertet oder veröffentlicht werden.

Abschrift der §§ 2 Nr. 1; 4; 23 GeschGehG

§ 2 GeschGehG – Begriffsbestimmungen

Im Sinne dieses Gesetzes ist

1. Geschäftsgeheimnis eine Information
 - a) die weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne Weiteres zugänglich ist und daher von wirtschaftlichem Wert ist und

Merkblatt zur Wahrung gesetzlicher Bestimmungen zur Geheimhaltung

- b) die Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist und
 - c) bei der ein berechtigtes Interesse an der Geheimhaltung besteht;
- (...)

§ 4 GeschGehG – Handlungsverbote

- (1) Ein Geschäftsgeheimnis darf nicht erlangt werden durch
 - 1. unbefugten Zugang zu, unbefugte Aneignung oder unbefugtes Kopieren von Dokumenten, Gegenständen, Materialien, Stoffen oder elektronischen Dateien, die der rechtmäßigen Kontrolle des Inhabers des Geschäftsgeheimnisses unterliegen und die das Geschäftsgeheimnis enthalten oder aus denen sich das Geschäftsgeheimnis ableiten lässt, oder
 - 2. jedes sonstige Verhalten, dass unter den jeweiligen Umständen nicht dem Grundsatz von Treu und Glauben unter Berücksichtigung der anständigen Marktgepflogenheit entspricht.
- (2) Ein Geschäftsgeheimnis darf nicht nutzen oder offenlegen, wer
 - 1. das Geschäftsgeheimnis durch eine eigene Handlung nach Absatz 1
 - a) Nummer 1 oder
 - b) Nummer 2
 erlangt hat,
 - 2. gegen eine Verpflichtung zur Beschränkung der Nutzung des Geschäftsgeheimnisses verstößt oder
 - 3. gegen eine Verpflichtung verstößt, das Geschäftsgeheimnis nicht offenzulegen.
- (3) Ein Geschäftsgeheimnis darf nicht erlangen, nutzen oder offenlegen, wer das Geschäftsgeheimnis über eine andere Person erlangt hat und zum Zeitpunkt der Erlangung, Nutzung oder Offenlegung weiß oder wissen müsste, dass diese das Geschäftsgeheimnis entgegen Absatz 2 genutzt oder offengelegt hat. Das gilt insbesondere, wenn die Nutzung in der Herstellung, dem Anbieten, dem Inverkehrbringen oder der Einfuhr, der Ausfuhr oder der Lagerung für diese Zwecke von rechtsverletzenden Produkten besteht.

§ 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, das ihr im Rahmen des Beschäftigungsverhältnisses anvertraut worden oder zugänglich geworden 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 Förderung 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.

Merkblatt zur Wahrung gesetzlicher Bestimmungen zur Geheimhaltung

- (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 Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.

Abschrift des § 3 TTDSG und des § 206 StGB

§ 3 TTDSG – 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 geschäftsmäßig 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 dürfen 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 dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich 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 bekannt geworden 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 Ermächtigungen mit dem Erbringen von Post- oder Telekommunikationsdiensten betraut sind oder
 3. mit der Herstellung einer dem Betrieb eines solchen Unternehmens dienenden Anlage oder mit dem 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

Merkblatt zur Wahrung gesetzlicher Bestimmungen zur Geheimhaltung

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.