

Geheimhaltungsvereinbarung

Die Auftraggeberin / der Auftraggeber wurde heute über Verschwiegenheits- und Sorgfaltspflichten im Zusammenhang mit ihrer/seiner Tätigkeit bzw. ihrem/seinem Aufenthalt unterrichtet.

Anschließend wurde sie/er

1. auf die Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutzgrundverordnung (DSGVO) und dem Bundesdatenschutzgesetz-Neu (BDSG-Neu),
2. zur Verschwiegenheit betreffend aller mit der Tätigkeit für und/oder bei dem Unternehmen zusammenhängenden Informationen sowie
3. zum sorgfältigen Umgang mit Informationstechniken (insbesondere mit dem Computer) verpflichtet. Diese Verpflichtungen bestehen gegenüber **jedermann** (d. h. auch gegenüber Mitarbeiter(innen)n des Unternehmens sowie gegenüber Familienangehörigen oder Freunden), soweit nicht eine dienstliche Veranlassung zur Offenlegung besteht. Auch nach Beendigung der Tätigkeit bestehen sie unbegrenzt fort.

Erläuterungen

zu **1. (Datenschutz)**: Es ist untersagt, personenbezogene Daten unbefugt zu verarbeiten.

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 festgelegt und beinhalten im Wesentlichen folgende Voraussetzungen:

Personenbezogene Daten müssen

- auf rechtmäßige Weise und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden;
- für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden;
- dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
- 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;
- 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;
- 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“).

Im Sinne von Art. 4 Nr. 1 DSGVO sind personenbezogene Daten 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 zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, der Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

„Verarbeiten“ im Sinne von Art. 4 Nr. 2 DSGVO ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte 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.

zu **2. (Verschwiegenheit)**: Der/die Unterzeichner(in) ist zur Geheimhaltung aller Informationen verpflichtet, die ihr/ihm im Zusammenhang mit ihrer/seiner Tätigkeit bzw. ihrem/seinem Aufenthalt bei dem Unternehmen bekannt werden bzw. bekannt geworden sind (entsprechend §§ 2, 4, 23 GeschGehG) und die nicht offenkundig sind. Dazu zählen insbesondere Geschäfts- und Betriebsgeheimnisse, wirtschaftliche Verhältnisse des Unternehmens oder der Geschäftspartner des Unternehmens, persönliche oder wirtschaftliche Verhältnisse der Mitarbeiter(innen) des Unternehmens, technische Spezifikationen, Verfahren etc.

zu **3. (sorgfältiger Umgang mit Informationstechniken)**: Nicht ordnungsgemäß erworbene bzw. lizenzierte Versionen von Computersoftware können einen Verstoß gegen das Urheberrecht bedeuten. Sie können sowohl das Unternehmen als auch die Personen, die die Software einsetzen, in straf- und zivilrechtliche Haftung bringen. Darüber hinaus besteht die Gefahr, dass getarnte Schadenssoftware (z. B. Viren, Trojaner, Spy-Programme) durch Verwendung illegaler Softwarekopien auf betriebliche PCs geladen wird oder dass andere Funktionsstörungen hervorgerufen werden. Die Risiken für schwere Schäden aufgrund von Computerviren und anderen schadenstiftenden Programmen erfordern die strikte Beachtung folgender Grundsätze:

- In den Netzen des Unternehmens darf nur Software genutzt werden, die von dem Unternehmen zur Verfügung gestellt worden ist. Es ist untersagt, externe Software zum Einsatz zu bringen.
- Das Kopieren von Software - insbesondere zum Zwecke des Betriebes auf fremder oder anderer firmeneigener Hardware - ist nicht gestattet.
- Generell unzulässig sind folgende vorsätzlich oder fahrlässig vorgenommene Handlungen:
 1. Das Abrufen oder Verbreiten von Inhalten, die gegen gesetzliche Bestimmungen verstoßen oder Persönlichkeitsrechte beeinträchtigen.
 2. Der Versand von Mitteilungen, die geeignet sind, beim Empfänger eine gewollte Schädigung an seiner Arbeit oder seinem System zu verursachen.
 3. Der Versand von Mitteilungen, der zur Überlastung der Systeme oder des Netzwerkes beiträgt oder anderweitig die Arbeit Dritter (hierzu zählen auch Mitarbeiter(innen) des Unternehmens) beeinträchtigt.
 4. Die Weitergabe von Passwörtern sowie die Verwendung von Passwörtern Dritter.
 5. Der Versuch, unberechtigten Zugang zu Ressourcen, Programmen oder Daten Dritter zu erlangen.
 6. Die Angabe einer falschen Identität gegenüber Dritten bei der Nutzung des Internets oder des Netzwerkes.
 7. Die Nutzung nicht von dem Unternehmen freigegebener IT-Geräte (z. B. Laptops) im internen Netzwerk des Unternehmens ist nicht gestattet!

8. Der Zugang zum E-Mailsystem des Unternehmens Gruppe und zum Internet wird über von dem Unternehmen zur Verfügung gestellte Geräte realisiert und dient ausschließlich der Kommunikation und Information im Interesse des Unternehmens; eine private Nutzung ist nicht gestattet. Gleiches gilt entsprechend für die Verwendung der Telefonanlage. Empfangene E-Mails mit privaten Inhalten sind unverzüglich zu entfernen oder an ein eigenes Postfach weiterzuleiten.
9. Sämtliche zur Verfügung gestellten Unterlagen und Arbeitsmittel (einschließlich zur Verfügung gestellter EDV-Hard- und Software) sind während der Dauer des Aufenthalts bzw. des Vertragsverhältnisses auf Anforderung und nach Beendigung des Aufenthalts bzw. des Vertragsverhältnisses unaufgefordert zurückzugeben.

Belehrungen

Verstöße gegen Geheimhaltungs- oder Datenschutzvorschriften können zivilrechtlich sowie strafrechtlich

- insbesondere nach dem Gesetz zum Schutz von Geschäftsgeheimnissen (**GeschGehG**)
- nach Art. 83 **DSGVO**, §§ 42 und 43 **BDSG**-Neu (Adressat ist hier unser Unternehmen) verfolgt bzw. geahndet werden. Ein Verstoß kann zugleich eine Verletzung von arbeitsvertraglichen Pflichten darstellen. Die unzulässige oder unrichtige Verarbeitung personenbezogener Daten kann nach Art. 82 DSGVO (Adressat ist hier unser Unternehmen) zu Haftungsansprüchen der betroffenen Person(en) führen. Die Verwendung illegaler Software kann ebenfalls zivilrechtlich sowie strafrechtlich
- insbesondere nach dem Urheberrecht (§ 106 UrhG) - verfolgt bzw. geahndet werden. Die Verbreitung von Schadenssoftware wird gemäß § 303b StGB strafrechtlich verfolgt. Im Übrigen ist der unbefugte Abruf geschützter Daten und die Zerstörung von Daten gemäß §§ 202a, 263a, 303a StGB ebenfalls strafbar.

Ein Auszug aus den genannten Rechtsvorschriften ist diesem Dokument als Anlage beigefügt.

Die Pflichtinformationen nach Art. 13 DSGVO über eine Verarbeitung Ihrer personenbezogenen Daten sowie über die Ihnen nach den datenschutzrechtlichen Regelungen zustehenden Ansprüche und Rechte können der ebenfalls beigefügten Anlage entnommen werden.

Mit meiner Unterschrift bestätige ich,

1. dass mir bekannt ist, dass es mir untersagt ist, personenbezogene Daten natürlicher Personen unbefugt – d. h. ohne Einwilligung der Person oder einer gesetzlichen Regelung – zu verarbeiten und dass die Verarbeitung nur in dem Umfang und in der Weise zulässig ist, wie es zur Erfüllung der mir übertragenen Aufgaben erforderlich ist;
2. dass mir bekannt ist, dass ich zur Geheimhaltung aller Informationen verpflichtet bin, die mir im Zusammenhang mit meiner Tätigkeit oder gelegentlich der Erfüllung meiner Tätigkeit bekannt werden bzw. bekannt geworden sind und die nicht offenkundig sind. Mir ist auch bekannt, dass hierzu insbesondere auch Geschäfts- und Betriebsgeheimnisse sowie persönliche oder wirtschaftliche Verhältnisse von Mitarbeiter(innen) des Unternehmens zählen;
3. dass mir bekannt ist, dass diese Verpflichtungen gegenüber jedermann bestehen, so auch gegenüber Familienangehörigen, Freunden oder gegenüber Arbeitskolleg(inn)en, soweit eine Mitteilung nicht aus dienstlichen Gründen erfolgt;
4. dass ich darüber belehrt wurde, dass ein Verstoß gegen das Datengeheimnis, die

Geheimhaltung oder der Einsatz nicht ordnungsgemäß erworbener bzw. lizenzierter Versionen von Software – insbesondere, wenn dadurch z. B. Schadenssoftware auf betriebliche Personal Computer geladen wird – gegebenenfalls mit Freiheits- oder Geldstrafen geahndet werden kann und dass Verstöße gegen jene Verpflichtungen Schadensersatzforderungen des Geschädigten auslösen können;

5. dass mir bekannt ist, dass diese Verpflichtungen auch nach Beendigung meiner Tätigkeit für das Unternehmen bzw. meines Aufenthalts fortbestehen;
6. dass mir ein Exemplar dieser Verpflichtungserklärung, Auszüge aus den wesentlichen Rechtsvorschriften sowie die Informationen nach Art 13 DSGVO ausgehändigt wurden.

Anlage

Bei Verstößen gegen die Verpflichtungserklärung werden folgende Gesetze berührt:

1. Datenschutzgrundverordnung (DSGVO)

• 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 öffentlichen Interesse 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 („Rechenschaftspflicht“).

• **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 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.

• **Art. 32 DSGVO (Sicherheit der Verarbeitung)**

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

- a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

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

(...)

• **Art. 82 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 Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

(...)

• **Art. 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.

(...)

(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:

(...)

(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:

(...)

2. Bundesdatenschutzgesetz-Neu (BDSG-Neu)

• § 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.

(...)

• § 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. Gesetz zum Schutz von Geschäftsgeheimnissen (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
 - 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, das 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.

(...)

4. Gesetz über Urheberrecht und verwandte Schutzrechte (UrhG)

§ 106 UrhG (Unerlaubte Verwertung urheberrechtlich geschützter Werke)

(1) Wer in anderen als den gesetzlich zugelassenen Fällen ohne Einwilligung des Berechtigten ein Werk oder eine Bearbeitung oder Umgestaltung eines Werkes vervielfältigt, verbreitet oder öffentlich wiedergibt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

5. Strafgesetzbuch (StGB)

• § 202 a 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.

• § 263 a StGB (Computerbetrug)

(1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, dass er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflusst, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(...)

• § 303 a StGB (Datenveränderung)

(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

(...)

• § 303 b StGB (Computersabotage)

(1) Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er

1. eine Tat nach § 303a Abs. 1 begeht,

2. Daten (§ 202a Abs. 2) in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt oder

3. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Handelt es sich um eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.

(3) Der Versuch ist strafbar.

(4) In besonders schweren Fällen des Absatzes 2 ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. einen Vermögensverlust großen Ausmaßes herbeiführt,
2. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Computersabotage verbunden hat,
3. durch die Tat die Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen oder die Sicherheit der Bundesrepublik Deutschland beeinträchtigt.