V e r p f l i c h t u n g s e r k l ä r u n g

für

Name, Vorname
Schule
Praktikumsbeginn

Ich verpflichte mich, das Bank- und Dienstleistungsgeheimnis zu wahren sowie die Vorschriften des Datenschutzgesetzes zu beachten.

Verpflichtung zur Vertraulichkeit nach der Datenschutzgrundverordnung (DS-GVO)

Verpflichtungserklärung
- Ich verpflichte mich zur Wahrung und Einhaltung der Vertraulichkeit.
- Ich werde zu keinem Zeitpunkt über diese Daten Dritten gegenüber Auskunft erteilen, sofern hierzu nicht kraft Gesetzes oder aus sonstigen Gründen eine entsprechende Verpflichtung besteht.
- Personenbezogene Daten werde ich nur im Einklang mit den datenschutzrechtlichen Grundsätzen verarbeiten. Hierzu zählen vor allem die Wahrung der Vertraulichkeit und die Rechtmäßigkeit der Verarbeitung.

Die Schweigepflicht gilt auch über die Dauer meines

☐ Tagesbetriebspraktikum

☐ Girl´s Day/Boy´s Day

hinaus.

Sofern es sich bei diesem Tag um keine schulische Veranstaltung handelt, haftet die Kreissparkasse Köln nicht für Unfälle, die auf dem Weg von und zur jeweiligen Einsatzstelle entstehen.

Aus versicherungsrechtlichen Gründen ist es für den o.a. Zeitraum nicht gestattet, Privatfahrten während der Dienstzeit zu unternehmen.

_____
Ort, Datum

_____ _____
Schüler/-in gesetzlicher Vertreter (beide Eltern)

Informationen zum vertraulichen Umgang mit Informationen
für Mitarbeiterinnen und Mitarbeiter

Verpflichtung zur Vertraulichkeit nach der Datenschutzgrundverordnung (DS-GVO)

Während Ihrer Tätigkeit kommen Sie mit personenbezogenen Daten insbesondere von anderen Mitarbeitern und Kunden der Sparkasse in Berührung. Personenbezogene Daten unterliegen einem besonderen gesetzlichen Schutz (/ vertraulicher Umgang). Es ist untersagt, personenbezogene Daten unbefugt zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu verarbeiten, z.B. durch erheben, erfassen, organisieren, ordnen, speichern, übermitteln, abfragen etc.

Eine Offenlegung, z.B. durch Weitergabe personenbezogener Daten – intern wie extern – ist nur zulässig, wenn dem Empfänger ein Recht auf Kenntnisnahme auf Grund einer Rechtsvorschrift zusteht oder die betroffene Person vorher eingewilligt hat.

Die Verpflichtungen bestehen auch nach Beendigung meiner Tätigkeit weiter, d.h. auch nach meinem Ausscheiden bei meinem Arbeitgeber.

Bei Fragen kann ich mich jederzeit an meine Führungskraft und an den Datenschutzbeauftragten meines Arbeitgebers wenden. Die Kontaktdaten sind im Intranet der Kreissparkasse Köln abrufbar.

Weitere Informationen zum Datenschutz finden Sie im „Merkblatt zur Verpflichtung zur Vertraulichkeit."

Auszüge der Artikel 5, 6, 9, 10, 22, 29, 82, 83 EU-DSGVO sowie §§ 42 BDSG-2017 und den §§ 202a-204, 206, 303a, 303b StGB sind dieser Belehrung zur Kenntnisnahme beigefügt.

Merkblatt zur Verpflichtung zur Vertraulichkeit nach der DS-GVO (Rechtsstand 26. Januar 2018)

Die Europäische Datenschutz-Grundverordnung (DS-GVO) gilt zusammen mit dem Bundesdatenschutzgesetz (BDSG-2017) für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, es sei denn, die Verarbeitung erfolgt durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten.

1. Grundbegriffe und Grundsätze der personenbezogenen Datenverarbeitung

Personenbezogene Daten sind 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.

Verarbeitung 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.

Bei allen Verarbeitungstätigkeiten mit Personenbezug sind stets die **Grundsätze** gemäß Artikel 5 DSGVO einzuhalten:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- Zweckbindung
- Datenminimierung, Richtigkeit, Speicherdauerbegrenzung
- Integrität und Vertraulichkeit
- Rechenschaftspflicht

2. Rechtmäßigkeit der personenbezogenen Datenverarbeitung

Eine Verarbeitungstätigkeit ist nur rechtmäßig, wenn mindestens eine der Bedingungen aus Artikel 6 DSGVO erfüllt ist, z.B. die **Einwilligung**, ein **Vertrag oder vorvertragliche Maßnahmen**, eine **rechtliche Verpflichtung**, der der Verantwortliche unterliegt, **lebenswichtige Interessen** oder **berechtigte Interessen** des Verantwortlichen, die die Interessen der Betroffenen **überwiegen**.
Anderenfalls ist die Verarbeitung untersagt („Verbot mit Erlaubnisvorbehalt“).

Die Verarbeitung besonderer Kategorien personenbezogener Daten –

- **rassische und ethnische Herkunft**
- **politische Meinungen**
- **religiöse oder weltanschauliche Überzeugungen**
- **Gewerkschaftszugehörigkeit**
- **genetischen Daten**
- **biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person**
- **Gesundheitsdaten**
- **Daten zum Sexualleben oder der sexuellen Orientierung** bzw.
- **Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln**

– ist **untersagt**, sofern nicht die Ausnahmen gemäß Artikel 9 bzw. Artikel 10 DS-GVO vorliegen.

Vor der Verarbeitung dieser Kategorien personenbezogener Daten ist eine **Rücksprache mit der Unternehmensleitung oder die Einholung des Rats des Datenschutzbeauftragten** erforderlich.

3. Automatisierte Entscheidungsfindung und Profiling

Besondere Voraussetzungen gelten auch bei der **automatisierten Entscheidungsfindung** – insbesondere wenn eine Entscheidung rechtliche Wirkung gegenüber der betroffenen Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt – sowie Profiling (Artikel 22 DS-GVO).

> **Profiling** ist die **Erfassung, Analyse, Bewertung und Vorhersage persönlicher Aspekte**, die sich auf eine natürliche Person beziehen, insbesondere **von (körperlicher, geistiger, wirtschaftlicher) Leistungsfähigkeit, Gesundheit, (tatsächlicher) (Arbeits-)Leistung und dem Verhalten, der Vorlieben, Interessen und der Aufenthaltsorte**.

Vor der Einführung oder Änderung dieser Verarbeitungsformen ist eine **Rücksprache mit der Unternehmensleitung oder die Einholung des Rats des Datenschutzbeauftragten** erforderlich.

Gesetzesauszüge (Rechtsstand 26. Januar 2018)

EU-Datenschutz-Grundverordnung

Art. 5 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 (… **„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 (… **„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. 6 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.
(…)
(4) Beruht die Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, nicht auf der Einwilligung der betroffenen Person oder auf einer Rechtsvorschrift (…), so berücksichtigt der Verantwortliche – um festzustellen, ob die Verarbeitung zu einem anderen Zweck mit demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist – unter anderem
a) jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung,
b) den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen,
c) die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Artikel 9 verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 verarbeitet werden,
d) die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,
e) das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann.

Art. 9 Verarbeitung besonderer Kategorien personenbezogener Daten
(1) Die Verarbeitung personenbezogener Daten, aus denen die **rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen** oder die **Gewerkschaftszugehörigkeit** hervorgehen, sowie die Verarbeitung von **genetischen Daten**, **biometrischen Daten** zur eindeutigen Identifizierung einer natürlichen Person, **Gesundheitsdaten** oder **Daten zum Sexualleben oder der sexuellen Orientierung** einer natürlichen Person ist **untersagt**.
(…)

Art. 10 Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten
Die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln aufgrund von Artikel 6 Absatz 1 darf nur unter behördlicher Aufsicht vorgenommen werden oder wenn dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, das geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorsieht, zulässig ist. Ein umfassendes Register der strafrechtlichen Verurteilungen darf nur unter behördlicher Aufsicht geführt werden.

Art. 22 Automatisierte Entscheidungen im Einzelfall einschließlich Profiling
(1) Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.
(…)

Art. 29 Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters
(… J)ede 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. 82 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.
(2) Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde.
(…)

Art. 83 Allgemeine Bedingungen für die Verhängung von Geldbußen

(4) Bei Verstößen gegen die folgenden Bestimmungen werden (…) **Geldbußen von bis zu 10.000.000 €** (… verhängt …):

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

(5) Bei Verstößen gegen die folgenden Bestimmungen werden (…) **Geldbußen von bis zu 20.000.000 €** (… verhängt …):

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

Bundesdatenschutzgesetz

§ 42 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.

Strafgesetzbuch

§ 202a 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 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 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.

(…)

§ 202d 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.

(…)

§ 203 Verletzung von Privatgeheimnissen

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,
2. Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlussprüfung,
3. Rechtsanwalt, Kammerrechtsbeistand, Patentanwalt, Notar, Verteidiger in einem gesetzlich geordneten Verfahren, Wirtschaftsprüfer, vereidigtem Buchprüfer, Steuerberater, Steuerbevollmächtigten oder Organ oder Mitglied eines Organs einer Rechtsanwalts-, Patentanwalts-, Wirtschaftsprüfungs-, Buchprüfungs- oder Steuerberatungsgesellschaft,
4. Ehe-, Familien-, Erziehungs- oder Jugendberater sowie Berater für Suchtfragen in einer Beratungsstelle, die von einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts anerkannt ist,
5. Mitglied oder Beauftragten einer anerkannten Beratungsstelle nach den §§ 3 und 8 des Schwangerschaftskonfliktgesetzes,
6. staatlich anerkanntem Sozialarbeiter oder staatlich anerkanntem Sozialpädagogen oder
7. Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen, steuerberaterlichen oder anwaltlichen Verrechnungsstelle

anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Amtsträger,
2. für den öffentlichen Dienst besonders Verpflichteten,
3. Person, die Aufgaben oder Befugnisse nach dem Personalvertretungsrecht wahrnimmt,
4. Mitglied eines für ein Gesetzgebungsorgan des Bundes oder eines Landes tätigen Untersuchungsausschusses, sonstigen Ausschusses oder Rates, das nicht selbst Mitglied des Gesetzgebungsorgans ist, oder als Hilfskraft eines solchen Ausschusses oder Rates,
5. öffentlich bestelltem Sachverständigen, der auf die gewissenhafte Erfüllung seiner Obliegenheiten auf Grund eines Gesetzes förmlich verpflichtet worden ist, oder
6. Person, die auf die gewissenhafte Erfüllung ihrer Geheimhaltungspflicht bei der Durchführung wissenschaftlicher Forschungsvorhaben auf Grund eines Gesetzes förmlich verpflichtet worden ist,

anvertraut worden oder sonst bekanntgeworden ist. Einem Geheimnis im Sinne des Satzes 1 stehen Einzelangaben über persönliche oder sachliche Verhältnisse eines anderen gleich, die für Aufgaben der öffentlichen Verwaltung erfasst worden sind; (…)

(4) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer unbefugt ein fremdes Geheimnis offenbart, das ihm bei der Ausübung oder bei Gelegenheit seiner Tätigkeit als mitwirkende Person oder als bei den in den Absätzen 1 und 2 genannten Personen tätiger Beauftragter für den Datenschutz bekannt geworden ist. Ebenso wird bestraft, wer

1. als in den Absätzen 1 und 2 genannte Person nicht dafür Sorge getragen hat, dass eine sonstige mitwirkende

Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind,

2. als im Absatz 3 genannte mitwirkende Person sich einer weiteren mitwirkenden Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, bedient und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind, oder

3. nach dem Tod der nach Satz 1 oder nach den Absätzen 1 oder 2 verpflichteten Person ein fremdes Geheimnis unbefugt offenbart, das er von dem Verstorbenen erfahren oder aus dessen Nachlass erlangt hat.

(5) Die Absätze 1 bis 4 sind auch anzuwenden, wenn der Täter das fremde Geheimnis nach dem Tod des Betroffenen unbefugt offenbart.

(6) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

§ 204 Verwertung fremder Geheimnisse

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein Betriebs- oder Geschäftsgeheimnis, zu dessen Geheimhaltung er nach § 203 verpflichtet ist, verwertet, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(…)

§ 206 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.

§ 303a 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.

(3) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.

§ 303b 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.

(5) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.