**Verpflichtungserklärung auf Vertraulichkeit und Verschwiegenheit**

**Datengeheimnis, Schweigepflicht (§ 203 StGB), Sozialgeheimnis (§ 35 SGB I), Fernmeldegeheimnis (§ 88 TKG) und Wahrung von Geschäftsgeheimnissen**

Frau/Herr (Vor-/Nachname) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

im Rahmen Ihrer Tätigkeit beim DRK-Musterverband e.V. als (zutreffendes bitte ankreuzen)

O Mitarbeiter/in (ink. Auszubildende, Praktikanten, Freiwilligendienstleistende)

O freiberufliche/r Mitarbeiter/in

O ehrenamtliche/r Mitarbeiter/in bzw. freiwillig Engagierte/r

O Beschäftigte/r der externen Firma (inkl. Lieferanten, Dienstleister)

 (Name/Adresse der Firma) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

kommen Sie mit personenbezogenen Daten und ggf. mit besonderen Kategorien personenbezogener Daten, wie z. B. Gesundheits- und Sozialdaten in Kontakt. Die einschlägigen gesetzlichen Vorschriften verlangen, dass alle Daten so verarbeitet werden, dass die Rechte der durch die Verarbeitung betroffenen Personen auf Vertraulichkeit und Integrität ihrer Daten gewährleistet werden. Daher ist es Ihnen auch nur gestattet, personenbezogene Daten in dem Umfang und in der Weise zu verarbeiten, wie es zur Erfüllung der Ihnen übertragenen Aufgaben erforderlich ist.

**1. Verpflichtung auf das Datengeheimnis**

1. Es ist Ihnen untersagt absichtlich oder unabsichtlich die Sicherheit der Verarbeitung in einer Weise zu verletzen, die zur Vernichtung, zum Verlust, zur Veränderung, zur unbefugten Offenlegung oder unbefugtem Zugang führt.
2. Personenbezogene Daten dürfen nur verarbeitet werden, wenn eine Einwilligung bzw. eine gesetzliche Regelung die Verarbeitung erlauben oder eine Verarbeitung dieser Daten vorgeschrieben ist und die Grundsätze der Verarbeitung eingehalten werden.
3. Verstöße gegen die Datenschutzvorschriften können ggf. mit Geldbuße, Geldstrafe oder Freiheitsstrafe geahndet werden. Entsteht der betroffenen Person durch die unzulässige Verarbeitung ihrer personenbezogenen Daten ein materieller oder immaterieller Schaden, kann ein Schadenersatzanspruch entstehen.
4. Ein Verstoß gegen die Vertraulichkeits- und Datenschutzvorschriften stellt einen Verstoß gegen arbeitsvertragliche Pflichten dar, der entsprechend geahndet werden kann. Diese Pflichten bestehen auch nach Beendigung Ihrer Tätigkeit fort.

**2. Verpflichtung auf die Wahrung der Vertraulichkeit und Verschwiegenheit**

Sofern Sie selbst gem. § 203 Strafgesetzbuch (StGB) als Berufsgeheimnisträger tätig sind oder aufgrund Ihrer Beschäftigung Tätigkeit eines Berufsgeheimnisträgers mitwirken, ist es Ihnen untersagt, fremde Geheimnisse, namentlich zum persönlichen Lebensbereich gehörende Geheimnisse oder Betriebs- oder Geschäftsgeheimnisse unbefugt zu offenbaren.

Ihre Schweigepflicht erstreckt sich auf alles, was Ihnen in Ausübung Ihrer Tätigkeit anvertraut oder bekannt geworden ist und bezieht sich auf alle schriftlichen Mitteilungen der Betroffenen, Aufzeichnungen über die betroffene Person und alle anderen Daten und Informationen über diese Person. Die Verschwiegenheitspflicht besteht gegenüber jedermann, so auch gegenüber Ihren eigenen Familienangehörigen, gegenüber Familienangehörigen der Betroffenen, gegenüber Arbeitskollegen/innen, soweit eine Mitteilung nicht aus erforderlichen dienstlichen Gründen erfolgt, gegenüber demjenigen, der von der betreffenden Tatsache bereits Kenntnis erlangt hat. Ihre Verschwiegenheitspflicht besteht auch nach dem Tod einer betroffenen Person fort.

**3. Verpflichtung auf die Wahrung des Sozialgeheimnisses**

Es kann nicht ausgeschlossen werden, dass Ihre Tätigkeit das Sozialgeheimnis gem. § 35 Sozialgesetzbuch erstes Buch (SGB I) berührt. Es ist Ihnen untersagt, unbefugt Sozialdaten zu erheben, zu verarbeiten oder zu nutzen. Sofern Daten verarbeitet werden, die dem Sozialgeheimnis unterliegen, haben Sie diese im gleichen Umfang geheim zu halten, wie die ursprünglich übermittelnde Stelle. Bitte beachten Sie, dass Verstöße gegen das Sozialgeheimnis ggf. mit Geldbuße, Geldstrafe oder Freiheitsstrafe geahndet werden können und einen Verstoß gegen arbeitsvertragliche Pflichten darstellen, der entsprechend geahndet werden kann. Diese Pflichten bestehen auch nach Beendigung Ihrer Tätigkeit fort.

**4. Verpflichtung auf Wahrung des Fernmeldegeheimnisses**

Unser Verband ist nach § 3 Abs. 2 TTDSG zur Einhaltung des **Fernmeldegeheimnisses** verpflichtet Dies schützt nicht nur die Inhalte, sondern auch die näheren Umstände der Telekommunikation, sondern auch die Information, ob jemand an einem Telekommunikationsvorgang beteiligt war, wann und wie lange eine Telekommunikation stattgefunden hat und auch die Umstände erfolgloser Verbindungsversuche. Dazu gehören nicht nur Telefonate und Faxe, sondern grundsätzlich auch die E-Mail-Kommunikation. Danach dürfen Sie unberechtigt weder sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste erforderliche Maß hinaus, Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation verschaffen noch derartige Kenntnisse grundsätzlich an Dritte weitergeben. Ein Verstoß gegen diese Bestimmung kann strafrechtlich verfolgt werden und kann gemäß § 206 Strafgesetzbuch eine Geldstrafe oder eine Freiheitsstrafe von bis zu fünf Jahren nach sich ziehen. Ebenfalls können arbeitsrechtliche Konsequenzen auf Sie zukommen.

**5. Verpflichtung auf Wahrung von Geschäftsgeheimnissen**

Im Rahmen Ihrer Tätigkeit erhalten Sie ggf. Kenntnis von Geschäfts- und Betriebsgeheimnissen. Diese sind im Interesse des Vereins besonders schützenswert. Es ist Ihnen daher untersagt, sich über das im Rahmen Ihrer Aufgaben erforderliche Maß hinaus Kenntnis von solchen Informationen zu verschaffen. Darüber hinaus ist es Ihnen verboten, solche Informationen an Unberechtigte weiterzugeben. Hierunter fallen auch Vorgänge von Drittunternehmen, mit denen Sie im Rahmen Ihrer Tätigkeit befasst sind. Alle Aufzeichnungen, Abschriften, Geschäftsunterlagen, Ablichtungen dienstlicher oder geschäftlicher Vorgänge, die Ihnen überlassen oder von Ihnen angefertigt werden, sind vor der Einsichtnahme unbefugter Personen zu schützen. Sie dürfen diese Unterlagen und Informationen auch nicht für eigene gewerbliche Zwecke nutzen. Hierbei ist es unerheblich, in welcher Form und auf welche Weise dies geschieht. Bei Verstößen können Sie sich unter Umständen gemäß § 17 des Gesetzes gegen den unlauteren Wettbewerb (UWG) strafbar machen. Dies kann eine Geldstrafe oder Freiheitsstrafe bis zu 5 Jahren nach sich ziehen. Ebenso können arbeitsrechtliche Konsequenzen bzw. Schadensersatzforderungen auf Sie zukommen.

Abschriften der genannten Vorschriften finden Sie in Auszügen auf dem beigefügten Merkblatt zum Datenschutz. Weitere, sich ggf. aus dem Arbeitsvertrag und/oder weiteren Anordnungen zu ergebende, allgemeine Geheimhaltungsverpflichtungen werden durch diese Erklärung nicht berührt.

**Bitte beachten Sie, dass diese Verpflichtung auf Vertraulichkeit und Verschwiegenheit
auch über die Beendigung des Beschäftigungsverhältnisses hinaus besteht.**

**Hiermit erkläre ich, dass ich die geltenden und zuvor genannten Vorschriften zur Vertraulichkeit und Verschwiegenheit einhalte. Das Merkblatt zum Datenschutz und ein Exemplar dieser Verpflichtung mit Anlage wurden mir ausgehändigt und ich habe es gelesen. Meine Fragen konnte ich stellen und sie wurden mir beantwortet.**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ort, Datum Unterschrift des/r Verpflichteten Ort, Datum Unterschrift des/r Verantwortlichen

**Anlage Merkblatt zum Datenschutz**

Sehr geehrte/r Mitarbeiter/in, liebe/r Ehrenamtliche/r,

es wäre sicherlich nicht in Ihrem Sinne, wenn Daten über Ihre Person und Ihre persönlichen Verhältnisse Unbefugten zur Kenntnis gelangen würden. Davor schützen Sie die verschiedenen gesetzlichen Regelungen zum Datenschutz.

Nach diesen Gesetzen sind auch Sie im Rahmen Ihrer beruflichen oder ehrenamtlichen Tätigkeit beim DRK dazu verpflichtet, die personenbezogenen Daten anderer vertraulich, rechtmäßig und weisungsgerecht zu behandeln. Bitte gehen Sie mit den Daten anderer mindestens so um, wie Sie Ihre eigenen Daten behandelt haben möchten.

Sie sind in Ihrer Tätigkeit dafür verantwortlich, dass die Ihnen anvertrauten personenbezogenen Daten nur im Rahmen Ihrer Aufgabenstellung verarbeitet (dazu gehören erheben, erfassen, organisieren, ordnen, speichern, anpassen oder verändern, auslesen, abfragen, verwenden, offenlegen durch Übermitteln, verbreiten oder in anderer Form bereitstellen, abgleichen oder verknüpfen, einschränken, löschen oder vernichten) oder genutzt werden.

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen. Als identifizierbar wird eine Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie z.B. einem Namen, zu einer Mitglieds- oder Personalnummer, zu Standortdaten wie Wohnanschrift oder Arbeitsstelle, zu einer Online-Kennung wie Benutzer-Account oder Mailadresse identifiziert werden kann. Jeder Missbrauch und jede unbefugte Weitergabe dieser Daten sind unzulässig und strafbar.

Die Datenschutzaufsichtsbehörde und betroffene Person kann jederzeit Auskunft verlangen, welche personenbezogene Daten Sie verarbeiten und welchem Zweck die Verarbeitung/Speicherung dient. Aus diesem Grund müssen Sie bzw. Ihr Verantwortlicher (Geschäftsführung, Vorstand) eine lückenlose Dokumentation der Datenverarbeitung nachweisen können.

Viren und Malware stellen ein erhebliches Sicherheitsrisiko dar. Umso wichtiger ist es daher, sicherzustellen, dass auf keinen Fall Viren von außen in das hausinterne Netzwerk eingeschleppt werden. Am häufigsten erfolgt eine „Infektion“ mit Computerviren durch die Verwendung von Wechseldatenträgern wie z.B. CDs, USB-Sticks mit Raubkopien und/oder sonstigen infizierten Datenbeständen oder über E-Mails aus nicht vertrauenswürdigen Quellen.

Insgesamt streben wir in unserem Hause einen gleichmäßigen Schutz aller Daten an – sowohl für die personenbezogenen Daten als auch für alle anderen sensiblen betriebsinternen Daten. Dies gilt ebenso für ihr häusliches und/oder mobiles Arbeitsumfeld.

**Im Rahmen Ihrer Tätigkeiten sind Sie unter anderem dafür verantwortlich, dass**

1. die Ihnen zur Verfügung gestellten Datenverarbeitungsgeräte /-programme aller Art sowie Ihr Passwort keinem Unbefugten zugänglich gemacht werden. Dies gilt sowohl für Akten und Schriftstücke als auch auf dem Bildschirm abrufbare Informationen. Bitte aktivieren Sie daher generell einen kennwortgeschützten Bildschirmschoner, bei längerer Abwesenheit ist es ratsam, sich ganz von dem System abzumelden.
2. die Büroräume bei Verlassen abgeschlossen sind und Aktenschränke mit sensiblen Daten stets
verschlossen sind.
3. Sie an Druckern und Faxgeräten keine Ausdrucke mit personenbezogenen Daten liegen lassen.
4. Sie nicht mehr benötigte Datenträger datenschutzgerecht vernichten, damit eine missbräuchliche Verwendung der Daten nicht mehr möglich ist.
5. Sie darauf achten, grundsätzlich sämtliche Daten auf den von Verlust und Manipulation gesicherten Server abzuspeichern. Steht z. B. beim mobilen Arbeiten kein Server zur Verfügung, können Daten für Bearbeitungszwecke kurzzeitig lokal gespeichert werden.

Bei Fragen zum Datenschutz oder in Zweifelsfragen wenden Sie sich als Mitarbeiter/in bitte direkt an Ihre/n Vorgesetzte/n und als Ehrenamtliche/r an ihre (fachliche) Ansprechperson.

**Anlage zur Verpflichtung auf Vertraulichkeit**

Die folgende Auswahl verschafft einen Überblick über datenschutzrechtliche und weitere gesetzliche Vorschriften. Die Darstellung erfolgt exemplarisch und ist keineswegs vollständig.

**Begrifflichkeiten der Datenschutz-Grundverordnung (DS-GVO)**

Art. 4 Nr. 1 DS-GVO: „**personenbezogene Daten“** [sind] 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;

Art. 9 DS-GVO: „**besondere Kategorien personenbezogener Daten**“ [sind] personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person;

Art. 4 Nr. 2 DS-GVO: „**Verarbeitung**“ [meint] 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. 33 Abs. 1 Satz 1 DS-GVO: 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.

**Grundsätze für die Verarbeitung personenbezogener Daten**

Personenbezogene Daten müssen

* auf rechtmäßige und in einer für die betroffene Person nachvollziehbaren Weise
verarbeitet werden (Art. 5 DS-GVO);
* 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;
* insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und der Aufwand nicht außer Verhältnis zum angestrebten Schutzzweck steht;
* sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein;
* 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.

Zudem sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf ihren Verarbeitungszweck unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

**Haftung und Schadenersatz**

Jede Person, der wegen eines Verstoßes gegen dieses Gesetz ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder Auftragsverarbeiter. Wegen eines Schadens, der nicht Vermögensschaden ist, kann die betroffene Person eine angemessene Entschädigung in Geld verlangen.

Verstößt ein Verantwortlicher oder ein Auftragsverarbeiter vorsätzlich oder fahrlässig gegen gesetzliche Bestimmungen, so kann die Datenschutzaufsichtsbehörde eine Geldbuße verhängen. Sie stellt sicher, dass die Geldbuße in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

**Auszug aus dem Telekommunikationsgesetz (TTDSG)**

**§ 3 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 Dienst 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 Telekommunikationsanalgen, 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 Verpflichteten ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder 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 Geheimnisses nicht gegenüber der Person, die das Fahrzeug führt oder gegenüber ihrer Stellvertretung.

**Auszug aus dem Gesetz gegen den unlauteren Wettbewerb (UWG)**

**§ 17 Verrat von Geschäfts- und Betriebsgeheimnissen**

(1) Wer als eine bei einem Unternehmen beschäftigte Person ein Geschäfts- oder Betriebsgeheimnis, das ihr im Rahmen des Dienstverhältnisses anvertraut worden oder zugänglich geworden ist, während der Geltungsdauer des Dienstverhältnisses unbefugt an jemand zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen, mitteilt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen,

1. sich ein Geschäfts- oder Betriebsgeheimnis durch

a) Anwendung technischer Mittel,

b) Herstellung einer verkörperten Wiedergabe des Geheimnisses oder

c) Wegnahme einer Sache, in der das Geheimnis verkörpert ist,

d) unbefugt verschafft oder sichert oder

2. ein Geschäfts- oder Betriebsgeheimnis, das er durch eine der in Absatz 1 bezeichneten
Mitteilungen oder durch eine eigene oder fremde Handlung nach Nummer 1 erlangt oder sich sonst unbefugt verschafft oder gesichert hat, unbefugt verwertet oder jemandem mitteilt.

(3) Der Versuch ist strafbar.

(4) In besonders schweren Fällen ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. gewerbsmäßig handelt,

2. bei der Mitteilung weiß, dass das Geheimnis im Ausland verwertet werden soll, oder

3. eine Verwertung nach Absatz 2 Nummer 2 im Ausland selbst vornimmt.

(5) 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.

(6) § 5 Nummer 7 des Strafgesetzbuches gilt entsprechend.

**Auszug aus dem Postgesetz (PostG)**

**§ 39 Postgeheimnis**

(1) Dem Postgeheimnis unterliegen die näheren Umstände des Postverkehrs bestimmter natürlicher oder juristischer Personen sowie der Inhalt von Postsendungen.

(2) Zur Wahrung des Postgeheimnisses ist verpflichtet, wer geschäftsmäßig Postdienste erbringt oder daran mitwirkt. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.

 (3) Den nach Absatz 2 Verpflichteten ist es untersagt, sich oder anderen über das für die Erbringung der Postdienste erforderliche Maß hinaus Kenntnis vom Inhalt von Postsendungen oder den näheren Umständen des Postverkehrs zu verschaffen. Sie dürfen Kenntnisse über Tatsachen, die dem Postgeheimnis 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 Postsendungen oder Postverkehr bezieht. Die Anzeigepflicht nach § 138 des Strafgesetzbuches hat Vorrang.

(4) Mitteilungen über den Postverkehr einer Person sind zulässig, soweit sie erforderlich sind, um Ansprüche gegen diese Person gerichtlich oder außergerichtlich geltend zu machen, die im Zusammenhang mit der Erbringung einer Postdienstleistung entstanden sind, oder um die Verfolgung von Straftaten zu ermöglichen, die beim Postverkehr zum Schaden eines Postunternehmens begangen wurden.

**Auszug aus dem Sozialgesetzbuch (SGB)**

**§ 35 SGB I Sozialgeheimnis**

Jeder hat Anspruch darauf, dass die ihn betreffenden Sozialdaten (§ 67 Abs. 1 Zehntes Buch) von den Leistungsträgern nicht unbefugt erhoben, verarbeitet oder genutzt werden (Sozialgeheimnis). Die Wahrung des Sozialgeheimnisses umfasst die Verpflichtung, auch innerhalb des Leistungsträgers sicherzustellen, dass die Sozialdaten nur Befugten zugänglich sind oder nur an diese weitergegeben werden. Sozialdaten der Beschäftigten und ihrer Angehörigen dürfen Personen, die Personalentscheidungen treffen oder daran mitwirken können, weder zugänglich sein noch von Zugriffsberechtigten weitergegeben werden. Die Beschäftigten haben auch nach Beendigung ihrer Tätigkeit bei den genannten Stellen das Sozialgeheimnis zu wahren.

**§ 78 SGB X Zweckbindung und Geheimhaltungspflicht eines Dritten, an den Daten übermittelt werden**

(1) Personen oder Stellen, die nicht in § 35 des Ersten Buches genannt und denen Sozialdaten übermittelt worden sind, dürfen diese nur zu dem Zweck verarbeiten oder nutzen, zu dem sie ihnen befugt übermittelt worden sind. Die Dritten haben die Daten in demselben Umfang geheim zu halten wie die in § 35 des Ersten Buches genannten Stellen. Sind Sozialdaten an Gerichte oder Staatsanwaltschaften übermittelt worden, dürfen diese gerichtliche Entscheidungen, die Sozialdaten enthalten, weiter übermitteln, wenn eine in § 35 des Ersten Buches genannte Stelle zur Übermittlung an den weiteren Dritten befugt wäre. Abweichend von Satz 3 ist eine Übermittlung nach § 115 des Bundesbeamtengesetzes und nach Vorschriften, die auf diese Vorschrift verweisen, zulässig. Sind Sozialdaten an Polizeibehörden, Staatsanwaltschaften, Gerichte oder Behörden der Gefahrenabwehr übermittelt worden, dürfen diese die Daten unabhängig vom Zweck der Übermittlung sowohl für Zwecke der Gefahrenabwehr als auch für Zwecke der Strafverfolgung und der Strafvollstreckung verarbeiten und nutzen.

**Auszug aus dem Strafgesetzbuch (StGB)**

**§ 202 Verletzung des Briefgeheimnisses**

(1) Wer unbefugt

1. einen verschlossenen Brief oder ein anderes verschlossenes Schriftstück, die nicht zu seiner Kenntnis bestimmt sind, öffnet oder

2. sich vom Inhalt eines solchen Schriftstücks ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wenn die Tat nicht in § 206 mit Strafe bedroht ist.

(2) Ebenso wird bestraft, wer sich unbefugt vom Inhalt eines Schriftstücks, das nicht zu seiner Kenntnis bestimmt und durch ein verschlossenes Behältnis gegen Kenntnisnahme besonders gesichert ist, Kenntnis verschafft, nachdem er dazu das Behältnis geöffnet hat

**§ 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.

**§ 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 der 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.

(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 Ordnungswidrigkeiten-verfahren 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.

**§ 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, dass ihm als

1. Person, die Aufgaben oder Befugnisse nach dem Personalvertretungsrecht wahrnimmt, anvertraut worden oder sonst bekanntgeworden ist.

(3) Kein Offenbaren im Sinne dieser Vorschrift liegt vor, wenn die in den Absätzen 1 und 2 genannten Personen Geheimnisse den bei ihnen berufsmäßig tätigen Gehilfen oder den bei ihnen zur Vorbereitung auf den Beruf tätigen Personen zugänglich machen. Die in den Absätzen 1 und 2 Genannten dürfen fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist; das Gleiche gilt für sonstige mitwirkende Personen, wenn diese sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit der in den Absätzen 1 und 2 Genannten mitwirken.

(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, dass 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.

**§ 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.