# Datenschutzverpflichtungserklärung - Anlage Merkblatt

## Merkblatt zur Vertraulichkeitsverpflichtung

**Hiermit werden Sie über Ihre Verantwortlichkeiten bezüglich personenbezogener Daten informiert und unterzeichnen eine Vertraulichkeitsvereinbarung. Dieses Merkblatt soll Ihnen einen Überblick über die wichtigsten Punkte geben. Bei Unklarheiten oder Fragen, insbesondere zur Zulässigkeit bestimmter Datenverarbeitungen, wenden Sie sich bitte an Ihren Vorgesetzten oder den Datenschutzbeauftragten unserer Organisation.**

### Datenschutz und Persönlichkeitsrecht

- **Zweck der Vertraulichkeitsverpflichtung:** Unsere Verpflichtung zum Datenschutz und Ihre diesbezügliche Vertraulichkeitserklärung dienen dem Schutz der Persönlichkeitsrechte der von den Daten betroffenen Personen. Diese Personen werden im Gesetz als "betroffene Personen" bezeichnet - dazu gehören z.B. Kunden, Kollegen und Sie als Mitarbeiter.
- **Persönlichkeitsrecht:** Jeder hat das Recht zu entscheiden, welche Informationen über ihn bekannt werden. Ein Kunde entscheidet beispielsweise, wer seine Adresse kennt, und Sie entscheiden, wer Informationen über Ihren Gesundheitszustand erhält.
- **Ausnahmen und Rechtfertigungen:** Es gibt Situationen, in denen es nicht allein auf den Willen der betroffenen Person ankommt. Jede solche Ausnahme bedarf jedoch einer gesetzlichen Rechtfertigung. Ein Beispiel hierfür ist die Regelung in Art. 6 Abs. 1 DS-GVO, wonach eine Einwilligung des Betroffenen oder eine gesetzliche Erlaubnis erforderlich ist. Eine häufige Rechtfertigung betrifft Daten, die für die Vertragserfüllung zwingend erforderlich sind. Ein Vermieter darf daher beispielsweise Ihren Namen speichern, ohne dass eine gesonderte Einwilligung Ihrerseits erforderlich ist.
- **Rechtlicher Rahmen:** Die Datenschutz-Grundverordnung (DS-GVO) ist in der gesamten Europäischen Union maßgeblich. Zusätzlich regelt das Bundesdatenschutzgesetz (BDSG) spezifische Fälle, insbesondere den Schutz von Mitarbeiterdaten.

### Ihre Vertraulichkeitsverpflichtung und der Umgang mit personenbezogenen Daten

**Grundlegende Verpflichtungen**

- Sie sind gesetzlich verpflichtet, personenbezogene Daten stets vertraulich zu behandeln. Das bedeutet, dass Sie diese Daten weder an unbefugte Dritte weitergeben noch ungeschützt zugänglich machen dürfen.
- Die Verarbeitung personenbezogener Daten, sei es das Lesen, Speichern, Löschen oder Übermitteln, ist nur zulässig, wenn eine entsprechende Erlaubnis vorliegt. Dies umfasst sowohl die gesetzliche Grundlage als auch die interne Aufgabenverteilung innerhalb unserer Organisation.

### Ihre persönliche Verantwortung

- Die Einhaltung der gesetzlichen Geheimhaltungspflichten, insbesondere nach Art. 29 DSGVO, ist nicht nur eine Verpflichtung unserer Organisation, sondern auch Ihre persönliche Verpflichtung. Die heutige Unterzeichnung einer Vertraulichkeitsvereinbarung unterstreicht die Bedeutung und Relevanz dieser Pflichten.

### Dauer und Reichweite der Vertraulichkeitsverpflichtung

- Ihre Verpflichtung zur Vertraulichkeit ist zeitlich unbegrenzt und besteht auch nach Beendigung Ihrer Tätigkeit für unser Unternehmen fort.
- Diese Verpflichtung erstreckt sich auf jeglichen Informationsaustausch mit Personen, die nicht ausdrücklich für den betreffenden Vorgang autorisiert sind, einschließlich anderer Mitarbeiter, Ihrer Familie und Medienvertretern.

### Anweisungen bei der Datenverarbeitung

- Beim Umgang mit personenbezogenen Daten haben Sie stets die Anweisungen Ihrer Vorgesetzten zu befolgen.

# Datenschutzverpflichtungserklärung - Anlage Merkblatt

## Der Begriff „personenbezogene Daten“

Das Datenschutzrecht bezieht sich auf alle „personenbezogenen Daten“. Nach Art. 4 Nr. 1 DS-GVO sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Das können zum Beispiel Informationen darüber sein, ob jemand Mitglied in einem Verein ist, wo er wohnt oder über welches Vermögen er verfügt.

Ein personenbezogenes Datum muss nicht unbedingt den Namen einer Person enthalten. Beispielsweise könnte die Information, dass das Konto mit der Nummer 123456 überzogen ist, als personenbezogen angesehen werden. Trotz des Fehlens eines Namens kann durch die Kombination verschiedener Daten schnell herausgefunden werden, wem das Konto gehört. Dies zeigt, dass es oft einfacher ist, eine Person zu identifizieren, als auf den ersten Blick vermutet. Die Forschungsergebnisse zeigen, dass mit Hilfe von Standortdaten zu elf verschiedenen Zeitpunkten jede von 1,5 Millionen Personen eindeutig identifiziert werden konnte.[1] Zudem konnten 87 Prozent der US-Amerikaner allein anhand von Geburtsdatum, Postleitzahl und Geschlecht eindeutig identifiziert werden.

Aus diesem Grund ist äußerste Vorsicht geboten: Selbst, wenn Sie davon ausgehen, dass bestimmte Daten keiner bestimmten Person zuzuordnen sind, dürfen Sie diese nicht ohne vorherige Zustimmung Ihres Vorgesetzten und des betrieblichen Datenschutzbeauftragten weitergeben oder veröffentlichen. Außerdem können diese Daten Betriebsgeheimnisse enthalten, die Sie ebenfalls streng vertraulich behandeln müssen.

## Anwendungsbereich des Datenschutzrechts

Das Datenschutzrecht bezieht sich nicht nur auf elektronisch verarbeitete Daten, wie sie in Computern und vielen technischen Geräten vorkommen. Entscheidend ist, dass es ebenfalls für „nichtautomatisierte Verarbeitung personenbezogener Daten gilt, die in einem Dateisystem erfasst oder für eine solche Erfassung vorgesehen sind“ gemäß Art. 2 Abs. 1 DS-GVO. Unter einem Dateisystem versteht man gemäß Art. 4 Nr. 6 DS-GVO jede strukturierte Sammlung von Daten, wie beispielsweise physische Patientenakten oder eine alphabetisch geordnete Ansammlung ausgefüllter Formulare. Darüber hinaus sind auch Daten erfasst, die aus einer Datei stammen oder für die spätere Ablage in einer solchen Datei bestimmt sind, wie z. B. eine ausgedruckte Kundenliste. Darüber hinaus schützt das Bundesdatenschutzgesetz (BDSG) Daten von Mitarbeitern oder Bewerbern in jeder Form. Dies gilt sogar für ungeordnete handschriftliche Notizen, die zur Entsorgung vorgesehen sind.

Wichtiger Hinweis: Die Speicherung der Telefonnummern von Freunden auf dem Handy ist weiterhin ohne besondere Rechtsgrundlage zulässig. Tätigkeiten, die rein persönlicher oder familiärer Natur sind, fallen nach Art. 2 Abs. 2 lit. c DS-GVO nicht unter das Datenschutzrecht.

## Verantwortlichkeiten in Bezug auf den Datenschutz

Sowohl unsere Organisation als auch Sie als Mitarbeiterinnen und Mitarbeiter sind nur dann berechtigt, personenbezogene Daten zu verarbeiten, wenn eine entsprechende **Rechtsgrundlage** vorliegt. Der Begriff der Verarbeitung nach Art. 4 Nr. 2 DS-GVO ist weit gefasst und umfasst jeden Umgang mit personenbezogenen Daten. Er reicht von der Erhebung bis zur Vernichtung der Daten. Art. 6 Abs. 1 DS-GVO nennt mögliche Rechtsgrundlagen, darunter die Einwilligung der betroffenen Person und verschiedene gesetzliche Erlaubnistatbestände.

Ihr Vorgesetzter informiert Sie darüber, welche Daten auf welcher Rechtsgrundlage verarbeitet werden dürfen. Beachten Sie: Die Verarbeitung abweichender Daten ist nicht zulässig. Darüber hinaus müssen personenbezogene Daten immer dem ursprünglich

[1] Vgl. Artikel „Bewegungsdaten von Mobiltelefonen: Individueller als der Fingerabdruck“, abrufbar unter: https://taz.de/Bewegungsdaten-von-Mobiltelefonen/!5070185/, zuletzt abgerufen: 09.08.2023.

festgelegten Zweck entsprechen. Jede Zweckänderung bedarf einer eigenen Rechtsgrundlage. So bedarf beispielsweise die Nutzung von Kundendaten, die bisher nur zur Vertragsabwicklung verwendet wurden, zu Werbezwecken einer gesonderten Erlaubnis. Auch hier wird Sie Ihr Vorgesetzter beraten.

Grundsätzlich gilt, dass Sie personenbezogene Daten niemals eigenmächtig weitergeben oder für eigene Zwecke nutzen dürfen.

Darüber hinaus sind Sicherheitsmaßnahmen für personenbezogene Daten unerlässlich. Diese schützen vor unberechtigtem Zugriff und unbeabsichtigtem Verlust. Aus diesem Grund verwenden wir bei der Online-Übertragung von Daten Verschlüsselungstechniken und führen regelmäßige Datensicherungen durch. Zahlreiche Sicherheitsmaßnahmen sind gesetzlich vorgeschrieben. Dazu gehört, dass Ausdrucke oder Datenträger nicht einfach entsorgt werden dürfen. Sie müssen entweder fachgerecht vernichtet oder von unserer IT-Abteilung sicher gelöscht werden.
Es sollte selbstverständlich sein, dass Sie Ihr persönliches Passwort nicht weitergeben oder sichtbar am Arbeitsplatz hinterlegen. Bei Missbrauch haften Sie persönlich für die Folgen, wie im Abschnitt „Folgen von Verstößen“ erläutert.

## Rechte der betroffenen Personen

Ein zentrales Element des Persönlichkeitsrechts besteht darin, **Kenntnis über gespeicherte Daten** zu haben. Daher muss eine Organisation, wenn sie Daten über eine Person erhebt, diese Person fast immer darüber informieren. Eine Person hat das Recht, von jeder Organisation eine **Kopie der über sie gespeicherten Daten** zu verlangen (Art. 15 DS-GVO). Dies bedeutet, dass alles, was Sie über einen Kunden notiert haben, diesem schriftlich zur Verfügung gestellt werden kann. Es ist daher wichtig, dass Sie nur Daten erfassen, für die Sie eine Erlaubnis zur Speicherung haben. Ihr Vorgesetzter wird Sie darüber informieren, welche Daten in Ihrem konkreten Fall zulässig sind. Achten Sie außerdem darauf, dass Sie Informationen präzise, objektiv und stets respektvoll festhalten. Daten dürfen grundsätzlich nicht an Dritte weitergegeben werden, es sei denn, es liegt eine ausdrückliche Genehmigung vor.

Nicht mehr benötigte Daten sind gemäß Art. 17 DS-GVO **zu löschen**. Unrichtige Daten sind gemäß Art. 16 DS-GVO **zu berichtigen**. Sollten Sie feststellen, dass nicht mehr benötigte Daten dennoch gespeichert sind, informieren Sie unverzüglich Ihren Vorgesetzten. Verstöße gegen diese Vorschrift können mit Geldbußen bis zu 20.000.000 Euro oder bis zu vier Prozent des weltweiten Jahresumsatzes geahndet werden, je nachdem, welcher Betrag höher ist. Geschädigte haben darüber hinaus Anspruch auf Schadenersatz einschließlich Schmerzensgeld.

Jeder Betroffene kann der Nutzung seiner Daten zu **Werbezwecken widersprechen** (Art. 21 Abs. 2, 3 und 5 DS-GVO) und hat in bestimmten Fällen ein **Widerspruchsrecht** (Art. 21 Abs. 1 DS-GVO).

Wenn Sie ein Auskunftsersuchen, einen Widerspruch oder andere datenschutzrelevante Anfragen erhalten, leiten Sie diese bitte **unverzüglich an den betrieblichen Datenschutzbeauftragten** weiter. Sie dürfen nur dann eigenständig tätig werden, wenn Ihnen diese Aufgabe ausdrücklich übertragen wurde. In Zweifelsfällen wenden Sie sich bitte an den betrieblichen Datenschutzbeauftragten. Bitte beachten Sie, dass auch Behörden oder die Polizei nicht ohne weiteres Daten von uns einsehen dürfen. Dazu ist ein förmlicher Beschlagnahmebeschluss erforderlich. Wenn Sie von einer Behörde kontaktiert werden, informieren Sie umgehend sowohl Ihren Vorgesetzten als auch den betrieblichen Datenschutzbeauftragten.

## Datenschutzrechtliche Verstöße und deren Konsequenzen

Verstöße gegen die Datenschutzbestimmungen können erhebliche Konsequenzen für unsere Organisation, aber auch für Sie persönlich haben. Die meisten dieser Verstöße können gemäß Art. 83 DS-GVO mit Geldbußen geahndet werden. Diese können bis zu 20 Millionen Euro pro Verstoß oder bis zu vier Prozent des weltweiten Jahresumsatzes unserer gesamten Organisation betragen, je nachdem, welcher Betrag höher ist.

Obwohl Strafen in dieser Höhe in der Regel für Organisationen vorgesehen sind, sollten Sie sich bewusst sein, dass in einigen Fällen auch Mitarbeiter direkt haftbar gemacht werden können. Der unsachgemäße Umgang mit personenbezogenen Daten, z. B. die Weitergabe ohne entsprechende Erlaubnis oder die Nutzung für eigene Zwecke, kann rechtliche Konsequenzen haben.

Einige Datenschutzverstöße sind zudem als Straftat eingestuft und können nach § 42 BDSG mit Freiheitsstrafe geahndet werden. Dies kann z.B. der Fall sein, wenn Datenträger mit sensiblen Informationen verkauft werden, anstatt sie ordnungsgemäß zu entsorgen. Auch andere Strafvorschriften wie § 202 a StGB (Ausspähen von Daten) oder § 263 a StGB (Computerbetrug) könnten zur Anwendung kommen.

Betroffene haben das Recht, bei unzulässiger Datenverarbeitung Schadensersatz, einschließlich Schmerzensgeld bei Persönlichkeitsrechtsverletzungen, nach Art. 82 DSGVO und §§ 823 ff. BGB geltend zu machen. Unter bestimmten Voraussetzungen können Sie persönlich für solche Schäden haftbar gemacht werden, insbesondere dann, wenn Sie die Daten rechtswidrig verwendet haben. Lassen Sie sich im Zweifelsfall von Ihrem Vorgesetzten oder dem Datenschutzbeauftragten beraten.

Ein weiterer wichtiger Faktor ist das Vertrauen unserer Kunden. Sollte ein Datenleck an die Öffentlichkeit gelangen, könnte dies das Kundenvertrauen nachhaltig schädigen. Nach Art. 34 Abs. 1 und Abs. 3 lit. c DSGVO könnten wir zudem verpflichtet sein, solche Vorfälle öffentlich zu machen oder die Betroffenen direkt zu informieren. Ihre Mitwirkung ist entscheidend, um solche Szenarien zu vermeiden.

Abschließend möchten wir Sie darauf hinweisen, dass Verstöße gegen Ihre Verschwiegenheitspflicht auch arbeitsrechtliche Konsequenzen haben können. Je nach Schwere des Verstoßes sind Sanktionen wie Abmahnungen oder sogar Kündigungen möglich.

## Neue Verfahren und die Verarbeitung personenbezogener Daten

Wenn Sie an einem Projekt arbeiten, bei dem personenbezogene Daten im Mittelpunkt stehen, ist es wichtig, den **betrieblichen Datenschutzbeauftragten von Anfang an zu konsultieren**. Der Datenschutzbeauftragte kann nicht nur die rechtlichen Rahmenbedingungen Ihres Vorhabens beurteilen, sondern auch wertvolle Hinweise zur Optimierung und Einhaltung der Vorgaben zu „Privacy by Design“ und „Privacy by Default“ (nach Art. 25 DSGVO) sowie zur Datensicherheit (nach Art. 32 DSGVO) geben. Eine frühzeitige Abstimmung erleichtert den Entwicklungsprozess und reduziert das Risiko unerwarteter rechtlicher Hürden. Sollte kein Datenschutzbeauftragter vorhanden sein, empfehlen wir, Ihre Vorgesetzten über etwaige Bedenken zu informieren.

Zu beachten ist, dass der Datenschutzbeauftragte gemäß Art. 38 Abs. 1 DSGVO rechtzeitig in alle datenschutzrelevanten Angelegenheiten einzubeziehen ist. Darüber hinaus kann es erforderlich sein, eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO durchzuführen und das entsprechende Verfahren nach Art. 30 DSGVO zu dokumentieren. Bei der Einbindung externer Dienstleister, z.B. für die Serveradministration, sind besondere Vereinbarungen nach Art. 28 DSGVO zu beachten.

Abschließend ist darauf hinzuweisen, dass unsere Organisation die konsequente Einhaltung der Datenschutzbestimmungen stets nachweisen muss (gem. Art. 5 und 24 DSGVO). Ein unzureichender Nachweis kann sowohl für die Organisation als auch für einzelne Mitarbeiter, die ein Verfahren ohne entsprechende Berechtigung durchführen, rechtliche Konsequenzen haben.

## Umgang mit Internet und E-Mail: Sicherheits- und Datenschutzhinweise

Das Internet und die E-Mail-Kommunikation bieten uns eine effiziente Möglichkeit, Informationen und Daten schnell zu übertragen. Während die meisten E-Mails heute während des Transports verschlüsselt sind, bleibt die Frage der End-to-End-Verschlüsselung, die den

Inhalt einer E-Mail über den gesamten Übertragungsweg schützt, eine wichtige Überlegung.

**Hauptregeln für sichere Kommunikation:**

1. **Vertraulichkeit:** Senden Sie keine sensiblen Daten ohne Zustimmung des Eigentümers per herkömmlicher E-Mail. Falls sowohl bei Ihnen als auch beim Empfänger End-to-End-Verschlüsselungssoftware verfügbar ist, können Sie sicher kommunizieren. Dennoch sollten Sie stets prüfen, ob die Datenübermittlung rechtlich zulässig ist.
2. **Richtige Adressierung:** Stellen Sie immer sicher, dass Ihre E-Mail an den beabsichtigten Empfänger geht. Ein sorgfältiges Überprüfen des Adressfeldes kann hierbei helfen, insbesondere wenn ähnliche Namen oder Adressen vorliegen.
3. **Adressfelder:** Der Unterschied zwischen „An:“, „CC:“ und „BCC:“ ist wesentlich:
    - An (To:): Hauptempfänger der E-Mail.
    - CC (Carbon Copy): Sekundäre Empfänger, die alle Informationen erhalten, jedoch nicht die Hauptzielgruppe der Nachricht sind.
    - BCC (Blind Carbon Copy): Empfänger, die nicht sichtbar sind für andere Empfänger. Dies ist besonders nützlich, wenn Sie die E-Mail-Adressen der Empfänger schützen möchten. Bei Massen-E-Mails konsultieren Sie bitte die EDV-Abteilung hinsichtlich geeigneter Versandmethoden.
4. **Externe Speicherung:** Es ist nicht gestattet, vertrauliche Daten an private E-Mail-Adressen weiterzuleiten oder sie außerhalb unserer Server zu speichern.
5. **Phishing-Versuche:** Bleiben Sie wachsam. Dank fortschrittlicher Technologien, wie künstlicher Intelligenz, werden Phishing-Mails immer überzeugender und schwerer zu erkennen. Selbst wenn eine E-Mail authentisch erscheint, klicken Sie nie auf verdächtige Links oder Anhänge. Bei Unsicherheiten sollten Sie sich an die EDV-Abteilung wenden, die E-Mail als Anhang weiterleiten und im Zweifel keine Aktionen basierend auf dieser E-Mail durchführen. Informieren Sie auch Ihre Kollegen über solche verdächtigen E-Mails, um das Bewusstsein im Team zu erhöhen.
6. **Vertrauenswürdigkeit von E-Mails:** Während digitale Signaturen ein höheres Vertrauensniveau bieten, sind sie noch nicht allgegenwärtig. Seien Sie trotzdem vorsichtig mit Anhängen, und öffnen Sie diese nur, wenn Sie den Absender kennen. Bei Unsicherheiten sollten Sie sich an die EDV-Abteilung wenden.
7. **Programmeinstellungen:** Änderungen, insbesondere bei den Sicherheitseinstellungen, sollten nicht ohne Absprache vorgenommen werden. Ihre Vorschläge und Bedenken können Sie immer an die EDV-Abteilung weitergeben.

## Erläuterungen zur Verpflichtung auf die Vertraulichkeit

**Die vorliegende Auswahl gesetzlicher Vorschriften soll Ihnen einen Überblick über das datenschutzrechtliche Regelwerk verschaffen. Die Darstellung erfolgt exemplarisch und ist keineswegs vollständig. Weitere Informationen zu datenschutzrechtlichen Fragestellungen erhalten Sie beim betrieblichen Datenschutzbeauftragten.**

### 1. Begrifflichkeiten

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 identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

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.

### 2. Begrifflichkeiten

Art. 5 Abs. 1 lit. a DS-GVO: Personenbezogene Daten müssen […] 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“).

Art. 5 Abs. 1 lit. f DS-GVO: Personenbezogene Daten müssen […] in einer Weise verarbeitet werden, die eine angemessene **Sicherheit** der personenbezogenen Daten gewährleistet, einschließlich Schutz vor **unbefugter oder unrechtmäßiger Verarbeitung** und vor unbeabsichtigtem **Verlust**, unbeabsichtigter **Zerstörung** oder unbeabsichtigter **Schädigung** durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).

Art. 29 DS-GVO: 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 Abs. 2 DS-GVO: 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 unbefugtem Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.

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.

### 3. Haftung

Art. 82 Abs. 1 DS-GVO: 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 Abs. 1 DS-GVO: Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von **Geldbußen** gemäß diesem Artikel für Verstöße gegen diese Verordnung […] in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

**§ 42 BDSG**

(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.

§ 202a Abs. 1 StGB: 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.

§ 303a Abs. 1 StGB: Wer rechtswidrig Daten […] löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

## 4. Optional – Fernmeldegeheimnis

**§ 3 TDDDG 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

- Anbieter von öffentlich zugänglichen Telekommunikationsdiensten sowie natürliche und juristische Personen, die an der Erbringung solcher Dienste mitwirken,
- Anbieter von ganz oder teilweise geschäftsmäßig angebotenen Telekommunikationsdiensten sowie natürliche und juristische Personen, die an der Erbringung solcher Dienste mitwirken,
- Betreiber öffentlicher Telekommunikationsnetze und
- 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.

### 5. Optional – Sozialgeheimnis

§ 78 Abs. 1 Satz 2 & 3 SGB X: […] [2]Eine Übermittlung von Sozialdaten an eine nicht-öffentliche Stelle ist nur zulässig, wenn diese sich gegenüber der übermittelnden Stelle verpflichtet hat, die Daten nur zu dem Zweck zu verarbeiten, zu dem sie ihr übermittelt werden. [3]Die Dritten haben die Daten in demselben Umfang geheim zu halten wie die in § 35 [SGB I] genannten Stellen.

### 6. Optional – Berufsgeheimnis

§ 203 StGB

(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. […]

(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. […]

**BRK-Kreisverband München**
Perchtinger Str. 5
81379 München
089 2373-285
servicestelle-ehrenamt@brk-muenchen.de
www.brk-muenchen.de