Mitarbeiterinformation zum Datenschutz

R.B.COM GmbH
Am Brünnele 2a
89291 Holzheim
Tel.: 07302 96330
Fax: 07303 963355
E-Mail: post@rbcom.de

I. Mitarbeiterinformation zur Benennung eines externen Datenschutzbeauftragten

Nach den Vorschriften des Gesetzes über die Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 (DSAnpUG-EU) haben wir uns entschlossen, einen externen Datenschutzbeauftragten (nachfolgend DSB genannt) zu benennen.

Mit Wirkung zum **18.01.2019** gemäß Art. 37 EU-Datenschutzgrundverordnung, in Verbindung mit § 38 Bundesdatenschutzgesetz, wird die

beOK IT solutions, Memminger Straße 59, 89264 Weißenhorn

zum betrieblichen Datenschutzbeauftragten benannt.

Die Aufgaben des DSB sind in Art. 39 der Europäischen Datenschutzgrundverordnung (DSGVO) grundsätzlich beschrieben. Zu seinen Aufgaben gehört insbesondere die
a) Unterrichtung und Beratung hinsichtlich der Pflichten nach dieser Verordnung sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedstaaten.
b) Überwachung der Einhaltung dieser Verordnung, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen.
c) Beratung (auf Anfrage) im Zusammenhang mit der Datenschutzfolgenabschätzung und Überwachung ihrer Durchführung gemäß Art. 35.
d) Zusammenarbeit mit der Aufsichtsbehörde.
e) Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Art. 36, und gegebenenfalls Beratung zu allen sonstigen Fragen.

Im Rahmen dieser gesetzlich normierten Pflichten bzw. Aufgaben ergeben sich folgende Detailaufgaben:
a) Durchführung von Prüfungen/Analysen über den Stand von Datenschutz und Datensicherung.
b) Beratung im Zusammenhang mit datenschutzrechtlich relevanten Verträgen und Vereinbarungen, z. B. bei Datenverarbeitung im Auftrag, Wartungsverträgen, Betriebsvereinbarungen u. a.
c) Beratungsaufgaben für die Verfahrensentwickler, Anwender, Benutzer und Betroffene.
d) Prüfung der Zulässigkeit von EDV-Verfahren und Festlegung von Auskunfts- und Benachrichtigungspflichten.
e) Überwachung der Beachtung der Rechte von Betroffenen.
f) Beratung bezüglich Hinweis- und Unterrichtungspflichten gegenüber Betroffenen, z. B. im Zusammenhang mit Werbung, Markt- und Meinungsforschung oder Übermittlung von Daten.

g) Beratung bei der Erarbeitung von Datenschutzregelungen und Verfahrensanweisungen zu den technischen und organisatorischen Maßnahmen des Datenschutzes und Kontrolle ihrer Einhaltung.
h) Führung des Verzeichnisses über die Verarbeitungstätigkeiten.
i) Kontrolle und ggf. Führung der Datenschutzdokumentation nach näherer Anweisung.

Diese Aufgaben werden freiverantwortlich in Abstimmung mit der Unternehmensleitung, ggf. auch auf Anforderung durch die verantwortlichen Fachbereiche, durchgeführt.

Der externe DSB ist für alle Beschäftigten und Betroffenen Ansprechpartner in allen betrieblichen Datenschutzfragen und ist über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, zur Verschwiegenheit verpflichtet, soweit er nicht durch den Betroffenen schriftlich von seiner Schweigepflicht entbunden worden ist. Er ist in der Ausübung seiner Fachkunde weisungsfrei und übt eine beratende Funktion aus.

Bei der Erfüllung seiner Aufgaben ist er von allen Mitarbeiterinnen und Mitarbeitern zu unterstützen und es sind ihm alle zur Wahrnehmung seiner Aufgaben erforderlichen Informationen und Unterlagen unverzüglich zur Verfügung zu stellen. Insbesondere ist der externe DSB über alle Datenverarbeitungsverfahren, in denen personenbezogene Daten verarbeitet werden, zu unterrichten und zur Berücksichtigung der datenschutzrechtlichen Anforderungen bei Verfahrensänderungen, Neuentwicklungen oder bei Beschaffungen umgehend in die Planung und Entwicklung einzuschalten.

Zur Unterstützung der Datenschutzarbeit, insbesondere zur Umsetzung des Datenschutzes im Unternehmen, werden in folgenden Unternehmensbereichen Datenschutzkoordinatoren benannt:
Fischer & Kollegen Steuerberatungsgesellschaft mbH & Co. KG, Frau Carola Götz

Datenschutzfragen, insbesondere Fragen zur Zulässigkeit der Erhebung, Verarbeitung oder Übermittlung personenbezogener Daten sind grundsätzlich über die zuständigen Abteilungsleiter bzw. den/die Datenschutzkoordinator/in dem DSB zur Stellungnahme zuzuleiten. In Einzelfällen, insbesondere bei persönlicher Betroffenheit, können sich die Mitarbeiterinnen und Mitarbeiter auch unmittelbar an den externen DSB wenden. Darüber hinaus können Datenschutzfragen auch vom bzw. über den Betriebsrat vorgelegt werden.
Der DSB ist wie folgt zu erreichen:

beOK IT solutions
Memminger Straße 59
89264 Weißenhorn
Tel.: 07309 4299200
Fax: 07309 4108081
E-Mail: datenschutz@beok-it.de

Der externe DSB ist der Geschäftsleitung unmittelbar unterstellt. Er berichtet quartalsweise an den Datenschutzkoordinator und einmal jährlich an die Geschäftsleitung. Für das Berichts- und Dokumentationswesen wird ein Datenschutzbericht erstellt und fortgeschrieben.

II. Vertraulichkeitsrichtline

1. Präambel

Der Schutz der Vertraulichkeit von personenbezogenen Daten von Beschäftigten, Kunden, Lieferanten und Geschäftspartnern ist im Hinblick auf die mögliche Verletzung des Persönlichkeitsrechts der Betroffenen und des damit eventuell verbundenen Schadens eine der zentralen Forderungen des Datenschutzes. Zu schützen sind aber in einem Unternehmen nicht nur die personenbezogenen Daten, sondern auch eine Reihe von weiteren vertraulichen Informationen und Daten des Unternehmens, bei deren Vertraulichkeitsverlust dem Unternehmen u. U. ein hoher Schaden entstehen kann.

Um eine vertrauliche Behandlung der zu schützenden Daten zu gewährleisten, ist es erforderlich, die zu schützenden Informationen und Daten zu identifizieren und falls notwendig zu kennzeichnen und den Umgang zu regeln. Das Anliegen der Vertraulichkeitsrichtlinien ist es deshalb, die im Unternehmen zu schützenden Informationen und Daten und deren Grad der Vertraulichkeit zu ermitteln und falls notwendig zu kennzeichnen, um damit allen Beschäftigten Verhaltensregeln zur Gewährleistung der Vertraulichkeit zur Verfügung zu stellen. Ziel dieser Vertraulichkeitsrichtlinie ist es aber auch, die Schutzbedürftigkeit der Ressource „Informationen und Daten“ bewusst zu machen und die Notwendigkeit des sorgfältigen Umgangs mit dieser Ressource zu verdeutlichen. Jeder Beschäftigte ist deshalb aufgerufen, im Interesse der Betroffenen und des Unternehmens und damit auch im eigenen Interesse, mit Informationen und Daten sorgfältig umzugehen und deren Vertraulichkeit zu wahren.

2. Zweck des Dokuments

Die im Unternehmen gespeicherten und verarbeiten Daten dienen unterschiedlichen Zwecken und unterliegen hinsichtlich ihrer Vertraulichkeit, der Integrität, Authentizität, Verfügbarkeit und Revisionsfähigkeit unterschiedlichen Ansprüchen. Da die Wahrung der Vertraulichkeit nicht zuletzt im Hinblick auf den Schutz des Persönlichkeitsrechts der Betroffenen und auch wegen ihrer Außenwirkung von besonderer Bedeutung ist und die Anforderungen an die Vertraulichkeit von der öffentlichen Zugänglichkeit von Informationen und Daten bis hin zu einer strengen Vertraulichkeit sehr unterschiedlich ausgeprägt sein können, wird der Schutz der Vertraulichkeit in dieser Richtlinie gesondert geregelt.

Mit dieser Richtlinie wird der Zweck verfolgt, alle relevanten und regelungsbedürftigen Informationen und Daten des Unternehmens zu identifizieren, ihren Schutzbedarf nach Vertraulichkeitsstufen zu ermitteln und die entsprechenden Datenbestände und Dokumente falls notwendig zu kennzeichnen sowie den Umgang damit zu regeln. Damit werden den Beschäftigten Leitlinien für den Umgang mit den Informationen und Daten zur Verfügung gestellt und eine unbeabsichtigte und irrtümliche Verletzung der Vertraulichkeit vermieden. Ferner ermöglicht die Klassifizierung der Informationen und Daten nach Vertraulichkeitsstufen eine sichere und fundierte Ableitung von angemessenen technischen und organisatorischen Maßnahmen zum Schutz der Vertraulichkeit und damit eine Verbesserung der Informationssicherheit im Unternehmen.

3. Geltungsbereich

→ Persönlicher Geltungsbereich

Diese Richtlinie gilt für alle Beschäftigten des Unternehmens und zusätzlich für externe und freie Mitarbeiter, Berater, etc., die Zugang zu Informationen und Daten besitzen, die dieser Richtlinie unterliegen.

→ Sachlicher Geltungsbereich

Diese Richtlinie gilt für alle personenbezogenen und sonstigen vertraulichen Informationen und Daten, die sich auf die Beschäftigten, Praktikanten sowie auf freie/externe Mitarbeiter und Berater etc. oder auf die Geschäftstätigkeit des Unternehmens beziehen, einschließlich aller Informationen und Daten, die das Unternehmen im Zusammenhang mit der Ausübung seiner Geschäftstätigkeit über Kunden, Geschäftspartner und Lieferanten etc. erhebt, speichert, verarbeitet, erzeugt und nutzt. Die Richtlinie gilt für alle Standorte und Niederlassungen.

4. Definition von Informationen und Medien

Informationen sind alle sinn- und werthaltigen Daten über die Beschäftigten, externe/freie Mitarbeiter, Praktikanten etc. des Unternehmens sowie über Kunden, Interessenten, Lieferanten, Geschäftspartner, Berater und sonstige Personen und Stellen, mit denen das Unternehmen in Verbindung steht und über die vom Unternehmen in Ausübung der Geschäftstätigkeit Daten erhoben, gespeichert, verarbeitet oder genutzt oder im Unternehmen generiert oder dem Unternehmen von diesen Stellen im Zusammenhang mit der Ausübung der Geschäftstätigkeit überlassen werden. Zu den Informationen zählen auch unternehmensinterne Dokumente und Dokumentationen wie Verzeichnisse, Systembeschreibungen, Handbücher und Richtlinien, Arbeitsanweisungen und Protokolle.

Unerheblich ist in diesem Zusammenhang, auf welchen Trägermedien die Informationen und Daten gespeichert sind. Unter diese Regelung fallen deshalb alle
a) codierten und uncodierten Daten in Datenbanken und Dateien,
b) elektronischen Dokumente unabhängig von der Art des Informationsträgers (PC, CD/DVD, USB-Sticks, Speicherkarten oder sonstige mobile Datenträger),
c) papierbasierten Dokumente,
d) Informationen auf Tonträgern und das gesprochene Wort sowie Bilder, unabhängig von der Art des Informationsträgers.

5. Rechte an den Informationen

Beim Umgang mit Informationen und Daten wird zwischen Informationseigentümern und Informationsnutzern unterschieden.

→ Informationseigentümer

Informationseigentümer sind alle Stellen im Unternehmen, in deren Verantwortungsbereich Informationen und Daten erhoben, gespeichert, verarbeitet und genutzt oder durch Verarbeitungsprozesse erzeugt oder denen Informationen und Daten von anderen Stellen zur Speicherung, Verarbeitung oder Nutzung in eigener Verantwortung übertragen bzw. übermittelt werden. Informationseigentümer sind z. B. der Leiter Personal oder der Leiter Vertrieb. Die informationsverantwortlichen Stellen ergeben sich aus der Arbeitsplatzbeschreibung, Geschäftsverteilungs- oder Organisationsplan.

Die Informationseigentümer sind befugt, für ihren Bereich (z. B. für bestimmte Teilbereiche, Projekte oder Kategorien von Informationen) weitere Informationseigentümer und deren Rechte festzulegen. Die Informationseigentümer legen den Vertraulichkeitsgrad für die einzelnen Informationen und Daten und den Kreis der Nutzungsberechtigten und deren Rechte falls notwendig fest. Sie legen ferner fest, an welche Empfänger oder Kategorien von Empfängern die Informationen und Daten innerhalb des Unternehmens offenbart und an welche Stellen außerhalb des Unternehmens sie übermittelt werden dürfen. Sie befinden ferner in Abstimmung mit dem IT-Sicherheitsverantwortlichen und ggf. dem Datenschutzbeauftragten über erforderliche technische und organisatorische Maßnahmen zur Wahrung der Vertraulichkeit der Informationen und Daten bei ihrer Erhebung, Speicherung, Verarbeitung, Nutzung oder Übertragung an andere Stellen (z. B. Verschlüsselung, Rechteprofile, Protokollierungen etc.). Die Informationen und Datenbestände sind in geeigneter Weise so nach dem Vertraulichkeitsgrad falls notwendig zu kennzeichnen, dass die Informationsnutzer im erforderlichen Umfang den Vertraulichkeitsgrad erkennen können.
Für Masseninformationen, insbesondere solche, deren Generierung, Verarbeitung, Nutzung und Offenbarung/Übermittlung in Geschäftsprozessen/Arbeitsabläufen vorgesehen ist, kann der Informationsverantwortliche Ausnahmen von der Kennzeichnungspflicht bestimmen. Diese von der Kennzeichnungspflicht ausgenommenen Informationen sind nach ihren Kategorien, Verarbeitungs-prozessen oder sonstigen geeigneten Kriterien oder Gruppenmerkmalen falls notwendig schriftlich festzulegen und zu regeln. Diese Informationen gelten als vertraulich.

→ Nutzungsberechtigte
Nutzungsberechtigte sind alle Personen und Stellen im Unternehmen, die befugt sind, im Rahmen ihrer vom Informationseigentümer festgelegten Berechtigungen Informationen und Daten zur Ausübung ihrer betrieblichen Aufgaben zur Kenntnis zu nehmen, zu verarbeiten, zu nutzen und zu übermitteln. Sie sind nicht befugt, die Informationen und Daten für andere als die zugewiesenen betrieblichen Aufgaben zu offenbaren oder zu übermitteln oder den Rahmen ihrer Berechtigungen oder den Vertraulichkeitsgrad der Informationen und Daten zu verändern. Zweifel an einer Offenbarungs- oder Übermittlungsbefugnis sind mit dem Informationseigentümer zu klären. Bis zur Klärung gelten die Informationen falls notwendig als vertraulich. Werden im Einzelfall im betrieblichen Interesse Abweichungen von den vorgegebenen Rechten erforderlich, sind diese mit dem Informationseigentümer abzustimmen.

6. Vertraulichkeitsgrade
Der Vertraulichkeitsgrad der Informationen und Daten richtet sich einerseits nach dem Risiko für die Interessen, Grundrechte und Grundfreiheiten der Betroffenen und dem Schaden, der dem Betroffenen bei einer Verletzung der Vertraulichkeit entstehen kann. Neben der datenschutzrechtlichen Bewertung sind auch die allgemeinen Vertraulichkeitsanforderungen für betriebswirtschaftliche Informationen und Daten als Grundlage zu berücksichtigen. Basis dieser Einstufung ist die Schutzstufeneinteilung nach den Regeln des Datenschutzhandbuchs. In die Beurteilung des möglichen Schadens sind auch die Eintrittswahrscheinlichkeit und ein eventuelles Wiederholungsrisiko des Schadensfalls einzubeziehen.

Folgende Vertraulichkeitsstufen werden festgelegt:
→ Öffentlich

Öffentliche Informationen und Daten sind für die Öffentlichkeit bestimmte und zur Veröffentlichung freigegebene oder öffentlich zur Verfügung gestellte Informationen und Daten, z. B. Presseveröffentlichungen oder Veröffentlichungen auf der Internetseite des Unternehmens.
Die Datenbestände, Informationsträger oder Schriftstücke/Dokumente sind falls notwendig mit dem Vermerk „Öffentlich“ zu kennzeichnen. Der Zugang zu diesen Informationen und Daten, die Nutzungsberechtigung und die Übermittlung an andere Stellen sind nicht eingeschränkt.

→ Intern

Die Informationen und Daten sind nur für den internen Gebrauch, aber nicht für die Öffentlichkeit bestimmt. Sie unterliegen intern keinen besonderen Zugangsbeschränkungen und dürfen intern allen Stellen und Personen offenbart werden. Ein Vertraulichkeitsverlust lässt i. d. R. keine oder keine nennenswerten Beeinträchtigungen der Interessen, Grundrechte und Grundfreiheiten der Betroffenen bzw. der betrieblichen Funktionen oder der Umweltbeziehungen des Unternehmens erwarten, z. B. Organisationspläne, Telefonverzeichnis etc.
Die Datenbestände, Informationsträger oder Schriftstücke/Dokumente sind falls notwendig mit dem Vermerk „Intern“ zu kennzeichnen. Der Zugang zu diesen Informationen und Daten und die Nutzungsberechtigung für interne betriebliche Zwecke sind nicht eingeschränkt, die Informationen und Daten dürfen aber nicht bzw. nur im Rahmen der Erfüllung der betrieblichen Aufgaben oder in Abstimmung mit dem Informationseigentümer an andere Stellen übermittelt werden.

→ Vertraulich

Die Informationen und Daten sind nur einem durch Geschäfts- oder Aufgabenverteilung bestimmbaren oder einem bestimmten, dem jeweiligen Zweck zugeordneten Personenkreis zugänglich, z. B. Beschäftigten einer bestimmten Abteilung oder Angehörigen von Projektteams. Ein Vertraulichkeitsverlust kann den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen oder den betrieblichen Funktionen bzw. Umweltbeziehungen des Unternehmens oder dessen Ansehen bei den Beschäftigten, den Kunden oder in der Öffentlichkeit erheblich schaden.
Die Datenbestände, Informationsträger oder Schriftstücke/Dokumente sind mit dem Vermerk „Vertraulich“ zu kennzeichnen. Der Zugang zu den Informationen ist nach Kategorien von Nutzungsberechtigten unter Regelung der Rechte an den Informationen und Daten sowie der Übermittlungsbefugnisse zu regeln. Ferner sind angemessene technische und organisatorische Maßnahmen zum Schutz der Vertraulichkeit festzulegen. Die Informationen und Daten dürfen intern nicht an andere Stellen offenbart und nur an festgelegte externe Empfänger (z. B. Vertragspartner, kooperierende Stellen oder Berater) übermittelt werden. Ausnahmen bedürfen der vorherigen Zustimmung durch den Informationseigentümer. Personaldaten sind grundsätzlich als vertraulich zu bewerten.

→ Streng vertraulich

Die Daten sind nur einem abgegrenzten, namentlich festgelegten Personenkreis zugänglich. Ein Vertraulichkeitsverlust kann den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigen oder die finanzielle oder marktwirtschaftliche Situation oder die Existenz des Unternehmens beeinträchtigen.
Die Datenbestände, Informationsträger oder Schriftstücke/Dokumente sind mit dem Vermerk „Streng vertraulich“ zu kennzeichnen. Der Kreis der Nutzungsberechtigten ist namentlich festzulegen. Interne

Offenbarungen oder Übermittlungen an andere Stellen sind nur durch den Informationseigentümer und nur im zwingend erforderlichen Umfang und nur gegen Nachweis der Offenbarung/Übermittlung zulässig. Darüber hinaus sind geeignete technische und organisatorische Maßnahmen zum Schutz der Vertraulichkeit der Informationen und Daten festzulegen, z. B. Verschlüsselung der Speicherung und Übertragung, Festlegung von befugten Empfängern, Regelung der Zulässigkeit der Herstellung von Kopien sowie deren Kontrolle, Verwaltung und Nachweisführung, und zur Aufbewahrung und Vernichtung.

7. Sonstige Regelungen

7.1 Unterschiedlicher Schutzbedarf innerhalb eines Datenbestands

Unterliegen Daten in einem nur einheitlich zu schützendem Datenbestand mit unterschiedlich hohen Vertraulichkeitsanforderungen, ist der gesamte Datenbestand nach den Anforderungen der am höchsten zu bewertenden Einzeldaten einzustufen.

7.2 Nachweis über streng vertrauliche Unterlagen

Jeder Informationseigentümer führt ein Verzeichnis über die in seinem Zuständigkeitsbereich vorhandenen streng vertraulichen Unterlagen. Soweit streng vertrauliche Unterlagen periodisch oder in gleicher Art wiederholt auftreten, z. B. Vorstandsprotokolle, ist es ausreichend, in dem Verzeichnis nur die Kategorien dieser Informationen zu bezeichnen.

7.3 Vertraulichkeitsverpflichtung

Informationseigentümer und Nutzer von streng vertraulichen Informationen werden durch eine zusätzliche schriftliche Erklärung zur Wahrung der strengen Vertraulichkeit verpflichtet.

7.4 Übermittlung von vertraulichen oder streng vertraulichen Informationen

Werden vertrauliche oder streng vertrauliche Informationen und Daten an andere Stellen im Unternehmen oder an externe Stellen übermittelt, sind diese Informationen mit folgendem Zusatz zu versehen:

Diese Informationen sind vertraulich/streng vertraulich und dürfen nur für die vereinbarten Zwecke genutzt werden. Eine Vervielfältigung der Informationen oder eine Weitergabe an andere Stellen ist nur mit der Einwilligung zulässig.

7.5 Generierung und Empfang von neuen Informationen

Werden vom Informationseigentümer oder von Informationsberechtigten neue Informationen generiert oder von anderen Stellen empfangen, sind diese Informationen nach den Regeln dieser Vertraulichkeitsrichtlinie zu klassifizieren und, soweit diese Informationen nicht von einer Kennzeichnungspflicht ausgenommen sind, nach ihrem Vertraulichkeitsgrad zu kennzeichnen. Zweifelsfragen sind mit dem zuständigen Informationseigentümer abzustimmen.

7.6 Änderung von Vertraulichkeitseinstufungen

Die Vertraulichkeitsanforderungen an Informationen können sich im Zeitablauf ändern. So kann ein Pressebericht während seiner Konzeptionsphase vertraulich sein, während er ab seiner Freigabe als „öffentlich“ zu bewerten ist.

Um einerseits den Aufwand für den Schutz von Informationen auf das erforderliche und angemessene Maß zu begrenzen, andererseits aber auch den erforderlichen Schutz der Informationen jederzeit zu

gewährleisten, ist bei einer Änderung der Vertraulichkeitsanforderungen die Einstufung der Vertraulichkeit anzupassen. Die Anpassung der Vertraulichkeitsstufe nimmt der Informationseigentümer vor bzw. ist mit dem Informationseigentümer abzustimmen. Die Informationsnutzer unterrichten den Informationseigentümer bei einer nicht mehr zutreffenden Kennzeichnung.

7.7 Fehlen einer Vertraulichkeitseinstufung

Ist eine klassifizierungspflichtige Information nicht nach ihrem Vertraulichkeitsgrad gekennzeichnet, ist diese Kennzeichnung unverzüglich nachzuholen. Bis zur Kennzeichnung gilt die Information als vertraulich. Alle Beschäftigten des Unternehmens sind verpflichtet, den zuständigen Informationseigentümer über eine fehlende Klassifizierung zu unterrichten.

7.8 Kennzeichnung der Informationen

Alle kennzeichnungspflichtigen Informationen sind untrennbar mit dem Klassifizierungsvermerk zu versehen. Bei Schriftstücken wird die Klassifikation falls notwendig in der Fußzeile oder durch Wasserzeichen angebracht. Sonstige Informationsträger werden durch einen entsprechenden Vermerk oder Stempelaufdruck gekennzeichnet. Einzelheiten regeln die Informationseigentümer für ihren Bereich.

7.9 Schutz der Informationen

Vertrauliche oder streng vertrauliche Informationen sind gegen Veränderungen zu schützen. Dies kann im einfachsten Fall durch einen Schreibschutz mit Passwort, durch Umwandlung in das PDF-Format und bei streng vertraulichen Dokumenten durch eine elektronische Signatur geschehen. Über die Art des Schutzes und über eventuelle Ausnahmen vom Dokumentenschutz entscheidet der Informationseigentümer.

III. Mitarbeiterinformation zur Vertraulichkeitsverpflichtung

1. Präambel

Im Zusammenhang mit der Erfüllung Ihrer betrieblichen Aufgaben erheben, verarbeiten und nutzen Sie personenbezogene Daten im Sinne der Europäischen Datenschutzgrundverordnung (DSGVO).

Personenbezogene Daten dürfen nach den Vorschriften der DSGVO nur erhoben, gespeichert, verarbeitet, genutzt oder übermittelt werden, soweit dies zur Erfüllung der Unternehmenszwecke erforderlich ist. In jeder Phase der Erhebung, Speicherung, Verarbeitung und Nutzung sind die personenbezogenen Daten vor unbefugtem Zugriff und unbefugter Kenntnisnahme sowie vor Verlust und Zerstörung zu schützen. Eine Übermittlung an Stellen außerhalb des Unternehmens ist nur zulässig, soweit dies zur Erledigung der betrieblichen Aufgaben erforderlich ist bzw. eine gesetzliche Offenbarungsbefugnis besteht. Auch innerhalb des Unternehmens ist eine Offenbarung gegenüber Kolleginnen und Kollegen nur zulässig, wenn die Kenntnis der Daten für deren Aufgabenerledigung erforderlich ist.

Eine Verletzung dieser Schutzpflichten kann Bußgeldforderungen und, soweit dem Betroffenen dadurch ein Schaden entstanden ist, auch Schadensersatzforderungen gegen das Unternehmen und im Rahmen der arbeitsrechtlichen Bestimmungen auch Regressforderungen gegen Sie auslösen. Personenbezogene Daten dürfen deshalb nur im Rahmen der betrieblichen Tätigkeit und nur zu dem zur jeweiligen rechtmäßigen oder arbeitsvertraglichen Aufgabenerfüllung gehörenden Zweck erhoben, verarbeitet, bekannt gegeben, zugänglich gemacht oder auf sonstige Weise genutzt werden. Geschützt sind alle personenbezogenen Daten, die unter Einsatz von Datenverarbeitungsanlagen verarbeitet, genutzt oder dafür erhoben werden oder aus diesen Datenverarbeitungsanlagen stammen. Geschützt sind aber auch Personalakten in jeder Form und diejenigen personenbezogenen Daten, die in nicht automatisierten Dateien verarbeitet werden, z. B. in herkömmlichen Karteien, Akten oder Aktensammlungen, wenn sie nach bestimmten Merkmalen zugänglich sind und ausgewertet werden können.

Das Datenschutzrecht, ausgestaltet in der Europäischen Datenschutzgrundverordnung und im Datenschutzanpassungs- und -Umsetzungsgesetz, ist ein Grundrecht und regelt den Schutz von personenbezogenen Daten bei der Erhebung, Speicherung, Verarbeitung, Nutzung und Übermittlung. Ein prägender Grundsatz des Datenschutzrechts ist, dass personenbezogene Daten nur erhoben, gespeichert, verarbeitet, genutzt und übermittelt werden dürfen, wenn ein Datenschutzgesetz oder eine andere Rechtsvorschrift dies erlaubt oder vorschreibt oder der Betroffene eingewilligt hat (Verbot mit Erlaubnisvorbehalt).

Verstöße gegen Datenschutzvorschriften können sowohl eine mit Bußgeld bedrohte Ordnungswidrigkeit als auch eine Straftat darstellen und nach arbeitsrechtlichen Vorschriften auch eine Schadensersatzpflicht des Arbeitnehmers begründen. Die Beachtung des Datenschutzes gehört deshalb zu den Vertragspflichten eines jeden Mitarbeiters in unserem Unternehmen. Bei Zweifelsfragen, insbesondere im Zusammenhang mit einer Offenbarung oder Übermittlung von personenbezogenen Daten an andere Stellen, wenden Sie sich bitte an Ihren Vorgesetzten oder an den betrieblichen Datenschutzbeauftragten. Unseren betrieblichen Datenschutzbeauftragten erreichen sie unter den nachstehenden Kontaktdaten. Der betriebliche Datenschutzbeauftragte ist seinerseits zur Vertraulichkeit verpflichtet und wird Ihre Anfragen vertraulich behandeln.

2. 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.

3. Grundsätze der Verarbeitung

→ 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 unbefugten 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.

4. 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

5. Rechtsgrundlagen
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 bei Ihrem Vorgesetzten und beim betrieblichen Datenschutzbeauftragten.

6. Strafvorschriften des § 42 DSAnpUG-EU (BDSG)
a) 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,

- einem Dritten übermittelt oder
- auf andere Art und Weise zugänglich macht

und hierbei gewerbsmäßig handelt.
b) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind,

- ohne hierzu berechtigt zu sein, verarbeitet oder
- durch unrichtige Angaben erschleicht

und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.
c) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind die betroffene Person, der Verantwortliche, die oder der Bundesbeauftragte und die Aufsichtsbehörde.

7. Fernmeldegeheimnis § 88 TKG
a) 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.

b) Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.
c) 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 Umstanden 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.

→ § 202a StGB Ausspähen von Daten
(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.
(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

→ § 203 StGB 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; Satz 1 ist jedoch nicht anzuwenden, soweit solche Einzelangaben anderen Behörden oder sonstigen Stellen für Aufgaben der öffentlichen Verwaltung bekanntgegeben werden und das Gesetz dies nicht untersagt.
(2a) (weggefallen)
(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, 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 StGB - 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.
(2) § 203 Absatz 5 gilt entsprechend.

→ § 206 StGB – Verletzung des Post- oder Fernmeldegeheimnisses

(1) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigten eines Unternehmens bekannt geworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft. (…)
(4) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die ihm als außerhalb des Post- oder Telekommunikationsbereichs tätigen Amtsträger aufgrund eines befugten oder unbefugten Eingriffs in das Post - oder Fernmeldegeheimnis bekannt geworden 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 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.

→ § 17 UWG – 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, 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 Nr. 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 Nr. 7 des Strafgesetzbuches gilt entsprechend.

§ 53 Zeugnisverweigerungsrecht der Berufsgeheimnisträger - Strafprozessordnung (StPO)
(1) Zur Verweigerung des Zeugnisses sind ferner berechtigt
1.Geistliche über das, was ihnen in ihrer Eigenschaft als Seelsorger anvertraut worden oder bekanntgeworden ist;
2.Verteidiger des Beschuldigten über das, was ihnen in dieser Eigenschaft anvertraut worden oder bekanntgeworden ist;
3.Rechtsanwälte und Kammerrechtsbeistände, Patentanwälte, Notare, Wirtschaftsprüfer, vereidigte Buchprüfer, Steuerberater und Steuerbevollmächtigte, Ärzte, Zahnärzte, Psychologische Psychotherapeuten, Kinder- und Jugendlichenpsychotherapeuten, Apotheker und Hebammen über das, was ihnen in dieser Eigenschaft anvertraut worden oder bekanntgeworden ist; für Syndikusrechtsanwälte (§ 46 Absatz 2 der Bundesrechtsanwaltsordnung) und Syndikuspatentanwälte (§ 41a Absatz 2 der Patentanwaltsordnung) gilt dies vorbehaltlich des § 53a nicht hinsichtlich dessen, was ihnen in dieser Eigenschaft anvertraut worden oder bekanntgeworden ist;
3a.Mitglieder oder Beauftragte einer anerkannten Beratungsstelle nach den §§ 3 und 8 des Schwangerschaftskonfliktgesetzes über das, was ihnen in dieser Eigenschaft anvertraut worden oder bekanntgeworden ist;
3b.Berater für Fragen der Betäubungsmittelabhängigkeit in einer Beratungsstelle, die eine Behörde oder eine Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts anerkannt oder bei sich eingerichtet hat, über das, was ihnen in dieser Eigenschaft anvertraut worden oder bekanntgeworden ist;
4.Mitglieder des Deutschen Bundestages, der Bundesversammlung, des Europäischen Parlaments aus der Bundesrepublik Deutschland oder eines Landtages über Personen, die ihnen in ihrer Eigenschaft als Mitglieder dieser Organe oder denen sie in dieser Eigenschaft Tatsachen anvertraut haben, sowie über diese Tatsachen selbst;
5.Personen, die bei der Vorbereitung, Herstellung oder Verbreitung von Druckwerken, Rundfunksendungen, Filmberichten oder der Unterrichtung oder Meinungsbildung dienenden Informations- und Kommunikationsdiensten berufsmäßig mitwirken oder mitgewirkt haben.

Die in Satz 1 Nr. 5 genannten Personen dürfen das Zeugnis verweigern über die Person des Verfassers oder Einsenders von Beiträgen und Unterlagen oder des sonstigen Informanten sowie über die ihnen im Hinblick auf ihre Tätigkeit gemachten Mitteilungen, über deren Inhalt sowie über den Inhalt selbst erarbeiteter Materialien und den Gegenstand berufsbezogener Wahrnehmungen. Dies gilt nur, soweit es sich um Beiträge, Unterlagen, Mitteilungen und Materialien für den redaktionellen Teil oder redaktionell aufbereitete Informations- und Kommunikationsdienste handelt.
(2) Die in Absatz 1 Satz 1 Nr. 2 bis 3b Genannten dürfen das Zeugnis nicht verweigern, wenn sie von der Verpflichtung zur Verschwiegenheit entbunden sind. Die Berechtigung zur Zeugnisverweigerung der in Absatz 1 Satz 1 Nr. 5 Genannten über den Inhalt selbst erarbeiteter Materialien und den Gegenstand entsprechender Wahrnehmungen entfällt, wenn die Aussage zur Aufklärung eines Verbrechens beitragen soll oder wenn Gegenstand der Untersuchung

1.eine Straftat des Friedensverrats und der Gefährdung des demokratischen Rechtsstaats oder des Landesverrats und der Gefährdung der äußeren Sicherheit (§§ 80a, 85, 87, 88, 95, auch in Verbindung mit § 97b, §§ 97a, 98 bis 100a des Strafgesetzbuches),

2.eine Straftat gegen die sexuelle Selbstbestimmung nach den §§ 174 bis 176, 177 Absatz 2 Nummer 1 des Strafgesetzbuches oder
3.eine Geldwäsche, eine Verschleierung unrechtmäßig erlangter Vermögenswerte nach § 261 Abs. 1 bis 4 des Strafgesetzbuches

ist und die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre. Der Zeuge kann jedoch auch in diesen Fällen die Aussage verweigern, soweit sie zur Offenbarung der Person des Verfassers oder Einsenders von Beiträgen und Unterlagen oder des sonstigen Informanten oder der ihm im Hinblick auf seine Tätigkeit nach Absatz 1 Satz 1 Nr. 5 gemachten Mitteilungen oder deren Inhalts führen würde.

§ 53a Zeugnisverweigerungsrecht der mitwirkenden Personen - Strafprozessordnung (StPO)
(1) Den Berufsgeheimnisträgern nach § 53 Absatz 1 Satz 1 Nummer 1 bis 4 stehen die Personen gleich, die im Rahmen

1.eines Vertragsverhältnisses,
2.einer berufsvorbereitenden Tätigkeit oder
3.einer sonstigen Hilfstätigkeit

an deren beruflicher Tätigkeit mitwirken. Über die Ausübung des Rechts dieser Personen, das Zeugnis zu verweigern, entscheiden die Berufsgeheimnisträger, es sei denn, dass diese Entscheidung in absehbarer Zeit nicht herbeigeführt werden kann.
(2) Die Entbindung von der Verpflichtung zur Verschwiegenheit (§ 53 Absatz 2 Satz 1) gilt auch für die nach Absatz 1 mitwirkenden Personen.

§ 97 StPO Beschlagnahmeverbot - Strafprozessordnung
(1) Der Beschlagnahme unterliegen nicht

1.schriftliche Mitteilungen zwischen dem Beschuldigten und den Personen, die nach § 52 oder § 53 Abs. 1 Satz 1 Nr. 1 bis 3b das Zeugnis verweigern dürfen;
2.Aufzeichnungen, welche die in § 53 Abs. 1 Satz 1 Nr. 1 bis 3b Genannten über die ihnen vom Beschuldigten anvertrauten Mitteilungen oder über andere Umstände gemacht haben, auf die sich das Zeugnisverweigerungsrecht erstreckt;
3.andere Gegenstände einschließlich der ärztlichen Untersuchungsbefunde, auf die sich das Zeugnisverweigerungsrecht der in § 53 Abs. 1 Satz 1 Nr. 1 bis 3b Genannten erstreckt.

(2) Diese Beschränkungen gelten nur, wenn die Gegenstände im Gewahrsam der zur Verweigerung des Zeugnisses Berechtigten sind, es sei denn, es handelt sich um eine elektronische Gesundheitskarte im Sinne des § 291a des Fünften Buches Sozialgesetzbuch. Die Beschränkungen der Beschlagnahme gelten nicht, wenn bestimmte Tatsachen den Verdacht begründen, dass die zeugnisverweigerungsberechtigte Person an der Tat oder an einer Datenhehlerei, Begünstigung, Strafvereitelung oder Hehlerei beteiligt ist, oder wenn es sich um Gegenstände handelt, die durch eine Straftat hervorgebracht oder zur Begehung einer Straftat gebraucht oder bestimmt sind oder die aus einer Straftat herrühren.

(3) Die Absätze 1 und 2 sind entsprechend anzuwenden, soweit die Personen, die nach § 53a Absatz 1 Satz 1 an der beruflichen Tätigkeit der in § 53 Absatz 1 Satz 1 Nummer 1 bis 3b genannten Personen mitwirken, das Zeugnis verweigern dürfen.

(4) Soweit das Zeugnisverweigerungsrecht der in § 53 Abs. 1 Satz 1 Nr. 4 genannten Personen reicht, ist die Beschlagnahme von Gegenständen unzulässig. Dieser Beschlagnahmeschutz erstreckt sich auch auf Gegenstände, die von den in § 53 Abs. 1 Satz 1 Nr. 4 genannten Personen den an ihrer

Berufstätigkeit nach § 53a Absatz 1 Satz 1 mitwirkenden Personen anvertraut sind. Satz 1 gilt entsprechend, soweit die Personen, die nach § 53a Absatz 1 Satz 1 an der beruflichen Tätigkeit der in § 53 Absatz 1 Satz 1 Nummer 4 genannten Personen mitwirken, das Zeugnis verweigern dürften.

(5) Soweit das Zeugnisverweigerungsrecht der in § 53 Abs. 1 Satz 1 Nr. 5 genannten Personen reicht, ist die Beschlagnahme von Schriftstücken, Ton-, Bild- und Datenträgern, Abbildungen und anderen Darstellungen, die sich im Gewahrsam dieser Personen oder der Redaktion, des Verlages, der Druckerei oder der Rundfunkanstalt befinden, unzulässig. Absatz 2 Satz 2 und § 160a Abs. 4 Satz 2 gelten entsprechend, die Beteiligungsregelung in Absatz 2 Satz 2 jedoch nur dann, wenn die bestimmten Tatsachen einen dringenden Verdacht der Beteiligung begründen; die Beschlagnahme ist jedoch auch in diesen Fällen nur zulässig, wenn sie unter Berücksichtigung der Grundrechte aus Artikel 5 Abs. 1 Satz 2 des Grundgesetzes nicht außer Verhältnis zur Bedeutung der Sache steht und die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes des Täters auf andere Weise aussichtslos oder wesentlich erschwert wäre.

§ 383 ZPO Zeugnisverweigerung aus persönlichen Gründen - Zivilprozessordnung
(1) Zur Verweigerung des Zeugnisses sind berechtigt:

1. der Verlobte einer Partei;
2.der Ehegatte einer Partei, auch wenn die Ehe nicht mehr besteht;
2a.der Lebenspartner einer Partei, auch wenn die Lebenspartnerschaft nicht mehr besteht;
3.diejenigen, die mit einer Partei in gerader Linie verwandt oder verschwägert, in der Seitenlinie bis zum dritten Grad verwandt oder bis zum zweiten Grad verschwägert sind oder waren;
4.Geistliche in Ansehung desjenigen, was ihnen bei der Ausübung der Seelsorge anvertraut ist;
5.Personen, die bei der Vorbereitung, Herstellung oder Verbreitung von periodischen Druckwerken oder Rundfunksendungen berufsmäßig mitwirken oder mitgewirkt haben, über die Person des Verfassers, Einsenders oder Gewährsmanns von Beiträgen und Unterlagen sowie über die ihnen im Hinblick auf ihre Tätigkeit gemachten Mitteilungen, soweit es sich um Beiträge, Unterlagen und Mitteilungen für den redaktionellen Teil handelt;
6.Personen, denen kraft ihres Amtes, Standes oder Gewerbes Tatsachen anvertraut sind, deren Geheimhaltung durch ihre Natur oder durch gesetzliche Vorschrift geboten ist, in Betreff der Tatsachen, auf welche die Verpflichtung zur Verschwiegenheit sich bezieht.

(2) Die unter Nummern 1 bis 3 bezeichneten Personen sind vor der Vernehmung über ihr Recht zur Verweigerung des Zeugnisses zu belehren.
(3) Die Vernehmung der unter Nummern 4 bis 6 bezeichneten Personen ist, auch wenn das Zeugnis nicht verweigert wird, auf Tatsachen nicht zu richten, in Ansehung welcher erhellt, dass ohne Verletzung der Verpflichtung zur Verschwiegenheit ein Zeugnis nicht abgelegt werden kann.

§ 384 ZPO Zeugnisverweigerung aus sachlichen Gründen - Zivilprozessordnung
Das Zeugnis kann verweigert werden:

1.über Fragen, deren Beantwortung dem Zeugen oder einer Person, zu der er in einem der im § 383 Nr. 1 bis 3 bezeichneten Verhältnisse steht, einen unmittelbaren vermögensrechtlichen Schaden verursachen würde;
2.über Fragen, deren Beantwortung dem Zeugen oder einem seiner im § 383 Nr. 1 bis 3 bezeichneten Angehörigen zur Unehre gereichen oder die Gefahr zuziehen würde, wegen einer Straftat oder einer Ordnungswidrigkeit verfolgt zu werden;
3.über Fragen, die der Zeuge nicht würde beantworten können, ohne ein Kunst- oder Gewerbegeheimnis zu offenbaren.

§ 84 Finanzgerichtsordnung (FGO)
(1) Für das Recht zur Verweigerung des Zeugnisses und die Pflicht zur Belehrung über das Zeugnisverweigerungsrecht gelten die §§ 101 bis 103 der Abgabenordnung sinngemäß.
(2) Wer als Angehöriger zur Verweigerung des Zeugnisses berechtigt ist, kann die Ableistung des Eides verweigern.

§ 104 Verweigerung der Erstattung eines Gutachtens und der Vorlage von Urkunden - Abgabenordnung (AO)
(1) Soweit die Auskunft verweigert werden darf, kann auch die Erstattung eines Gutachtens und die Vorlage von Urkunden oder Wertsachen verweigert werden. § 102 Abs. 4 Satz 2 bleibt unberührt.
(2) Nicht verweigert werden kann die Vorlage von Urkunden und Wertsachen, die für den Beteiligten aufbewahrt werden, soweit der Beteiligte bei eigenem Gewahrsam zur Vorlage verpflichtet wäre. Für den Beteiligten aufbewahrt werden auch die für ihn geführten Geschäftsbücher und sonstigen Aufzeichnungen.

→ § 78 Abs. 1 Satz 2 & 3 SGB X
(1) Personen oder Stellen, die nicht in § 35 des Ersten Buches genannt und denen Sozialdaten übermittelt worden sind, dürfen diese nur zu dem Zweck speichern, verändern, nutzen, übermitteln, in der Verarbeitung einschränken oder löschen, zu dem sie ihnen befugt übermittelt worden sind. Eine Übermittlung von Sozialdaten an eine nicht-öffentliche Stelle ist nur zulässig, wenn diese sich gegenüber der übermittelnden Stelle verpflichtet hat, die Daten nur für den Zweck zu verarbeiten, zu dem sie ihr übermittelt werden. 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 4 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 speichern, verändern, nutzen, übermitteln, in der Verarbeitung einschränken oder löschen.