

# Verpflichtung zur Wahrung der Vertraulichkeit und zur Beachtung des Datenschutzes

Die einschlägigen gesetzlichen Vorschriften verlangen, dass personenbezogene Daten so verarbeitet werden, dass die Rechte der durch die Verarbeitung betroffenen Personen auf Vertraulichkeit und Integrität ihrer Daten gewährleistet werden. Daher ist es mir auch nur gestattet, personenbezogene Daten in dem Umfang und in der Weise zu verarbeiten, wie es zur Erfüllung der mir übertragenen Aufgaben oder der Funktion erforderlich ist.

Nach diesen Vorschriften ist es untersagt, personenbezogene Daten unbefugt oder unrechtmäßig zu verarbeiten oder 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.

Verstöße gegen die Datenschutzvorschriften können seitens des Gesetzgebers ggf. mit Geldbuße, Geldstrafe oder Freiheitsstrafe geahndet werden und schwer bis nicht kalkulierbare Folgen für den Verein haben. Entsteht beispielsweise der betroffenen Person durch die unzulässige Verarbeitung ihrer personenbezogenen Daten ein materieller oder immaterieller Schaden, kann ein Schadenersatzanspruch gegen den Verein entstehen.

Ein Verstoß gegen die Vertraulichkeits- und Datenschutzvorschriften stellt somit auch einen Verstoß gegen Grundsätze des Vereins dar, der im schlimmsten Fall zu einer Schädigung des Vereins oder Dritten bzw. Einzelpersonen führen kann und der ggf. straf- und zivilrechtliche Konsequenzen haben kann. Ebenso ist als Folge ein Ausschluss aus dem Verein möglich.

Sollte im Rahmen meiner Aufgabe/Tätigkeit/Funktion ein Verstoß festgestellt werden, dann muss dieser unverzüglich dem Vorstand des Vereins persönlich oder per E-Mail (an [vorstand@schlagwerk.org](mailto:vorstand@schlagwerk.org)) mitgeteilt werden, damit Auswirkungen abgeschätzt als auch die Meldepflichten des Vereins an Behörden und datenschutzrelevante Stellen eingehalten werden können.

Es ist nicht ungewöhnlich, dass Fehler im Umgang mit Daten passieren.

Der Vorstand des Vereins möchte jedoch auf einen bewussten Umgang mit personenbezogenen Daten hinweisen und ermutigen, im Falle eines unsachgemäßen Umgangs den Schaden zu begrenzen, transparent zu kommunizieren, um daraus zu lernen und problematische Situationen in Zukunft zu vermeiden.

Meine Tätigkeit berührt das Fernmeldegeheimnis. Ich darf mir nicht über das erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation verschaffen. Ich darf derartige Kenntnisse grundsätzlich nicht an Dritte weitergeben.

Meine Tätigkeit berührt die Schweigepflicht. Es ist mir untersagt, fremde Geheimnisse, namentlich zum persönlichen Lebensbereich gehörende Geheimnisse unbefugt zu offenbaren.

Die Verpflichtung auf die Vertraulichkeit besteht auch nach der Beendigung der Tätigkeit für den Verein fort.

Ich, Name

Bereich/Funktion/Tätigkeit

\_\_\_\_\_

verpflichte mich, in Bezug auf die Vertraulichkeit und Integrität personenbezogener Daten, die Vorgaben der geltenden Datenschutzvorschriften einzuhalten und ausschließlich auf Weisung des Vereins zu verarbeiten.

Mit meiner Unterschrift bestätige ich zugleich den Empfang einer Kopie dieser Niederschrift nebst Anlage.

.....

Ort

Datum

.....

Verpflichtete(r)

# Anlage

## Erläuterungen zur Verpflichtung auf die Vertraulichkeit

Die vorliegende Auswahl gesetzlicher Vorschriften soll einen Überblick über das datenschutzrechtliche Regelwerk verschaffen. Die Darstellung erfolgt exemplarisch und ist keineswegs vollständig.

### 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 (Nickname), E-Mail Adresse 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. Die Datenschutzgesetze regeln den Schutz personenbezogener Daten bei deren Verarbeitung. Irrelevant ist dabei, ob diese Daten „digital“ (in Datenbanken, Dateien, IT-Systemen/-Applikationen etc.) oder „analog“ (Karteikarten, Akten etc.) verarbeitet werden.

### 2. 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, ein-

schließlich 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.

### 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. Fernmeldegeheimnis

§ 3 TTDSG<sup>1</sup>

(1) <sup>1</sup>Dem Fernmeldegeheimnis unterliegen der **Inhalt der Telekommunikation** und ihre **näheren Umstände**, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. <sup>2</sup>Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

Wichtig: Telekommunikation umfasst unter anderem auch Informationsaustausch per Messenger, SMS und E-Mail

(2) Zur Wahrung des Fernmeldegeheimnisses sind verpflichtet

1. Anbieter von öffentlich zugänglichen Telekommunikationsdiensten sowie natürliche und juristische Personen, die an der Erbringung solcher Dienste 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 Telekommunikationsanlagen, mit denen geschäftsmäßig Telekommunikationsdienste erbracht werden.

<sup>3</sup>Die Pflicht zur Geheimhaltung besteht auch **nach dem Ende der Tätigkeit** fort, durch die sie begründet worden ist.

(3) <sup>1</sup>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. <sup>2</sup>Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den in Satz 1 genannten Zweck verwenden.

<sup>3</sup>Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an

---

<sup>1</sup> Vormals § 88 TKG

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.[...]

## 5. 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. [...]

Stand: März 2022