

Verpflichtung auf die Vertraulichkeit nach DSGVO für festangestellte Mitarbeiter und Rechnungssteller

Datenschutz:

Die Datenschutzgesetze fordern, dass personenbezogene Daten so verarbeitet werden, dass die Rechte der Personen, deren Daten verarbeitet werden, auf Vertraulichkeit und Integrität ihrer Daten gewährleistet werden. Unzulässig ist es, 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 zu unbefugtem Zugang führt.

Im Rahmen deiner Tätigkeit erhältst du u.U. Zugang zu personenbezogenen Daten oder Kenntnis von solchen, etwa von Kollegen, Kunden oder anderen Personen. Du darfst personenbezogene Daten nur in dem Umfang und in der Weise verarbeiten, wie es zur Erfüllung der dir übertragenen Aufgaben erforderlich ist.

Verstöße gegen die Datenschutzvorschriften können ggf. mit Geldbuße, Geldstrafe oder Freiheitsstrafe geahndet werden. Entsteht der betroffenen Person durch die unzulässige Verarbeitung ihrer personenbezogenen Daten ein materieller oder immaterieller Schaden, kann ein Schadenersatzanspruch entstehen.

Ein Verstoß gegen die Vertraulichkeits- und Datenschutzvorschriften stellt einen Verstoß gegen vertragliche Pflichten dar, der entsprechend geahndet werden kann.

Fernmeldegeheimnis:

Soweit du im Rahmen deiner Aufgaben mit Telekommunikations-Daten in Berührung kommst (zum Beispiel auf administrativer Ebene E-Mail-Accounts verwalten, Internet-Kommunikationsdaten verarbeiten, Telefonanlagen oder IT-Netzwerktechnik betreuen, etc.), gilt zudem regelmäßig das Fernmeldegeheimnis. Dieses besagt, dass du dir nicht über das für die Erbringung der Telekommunikationsdienste einschließliche des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation verschaffen und du derartige Kenntnisse grundsätzlich nicht an Dritte weitergeben darfst. Bist du auf der Suche nach weiteren Informationen rund um den Datenschutz, dann wende dich als Rechnungssteller an deinen Ansprechpartner bei der dich beauftragenden Firma. Als festangestellter Mitarbeiter findest du darüber hinaus weitere Informationen im Intranet.

Außerdem kannst du dich bei Fragen zu den von dir für uns verarbeiteten Daten an datenschutz@bavaria-film.de wenden.

Verpflichtungserklärung:

Aufgrund deiner Aufgabenstellung und unter Hinweis auf vorstehende Erläuterungen verpflichten wir dich hiermit auf

- Einhaltung der Datenschutzgesetze, insbesondere darauf, personenbezogene Daten nicht unbefugt zu verarbeiten,
- die Wahrung der Vertraulichkeit personenbezogener Daten nach Art. 5 Abs. 1 lit. f) und Art. 32 DSGVO, zu denen du im Rahmen deiner Tätigkeiten Zugang erhältst oder Kenntnis erlangst,
- Soweit im Rahmen der Tätigkeit eine Verarbeitung von Telekommunikations-Daten vorkommen kann, ist weiterhin das Fernmeldegeheimnisses zu beachten., soweit dieses für dich im Rahmen der jeweiligen Tätigkeit relevant ist.

Wichtig: Diese Verpflichtung besteht auch nach Beendigung deiner Tätigkeit fort!

Für deine Unterlagen erhältst du folgende Dokumente:

- Anlage 1: Merkblatt zum Datenschutz
- Anlage 2: Auswahl gesetzlicher Vorschriften aus DSGVO und BDSG

Anlage 1 zur Verpflichtung auf die Vertraulichkeit

Merkblatt zum Datenschutz

Beim Umgang mit personenbezogenen Daten müssen neben anderen Gesetzen und Vorschriften vor allem die Bestimmungen der Europäischen Datenschutzgrundverordnung (DSGVO) und ergänzend des Bundesdatenschutzgesetzes (BDSG) beachtet werden. Zweck des Datenschutzes ist es, den Einzelnen davor zu schützen, dass durch den Umgang mit seinen personenbezogenen Daten seine Persönlichkeitsrechte beeinträchtigt werden. Verantwortliches Handeln beim Umgang mit personenbezogenen Daten ist damit entscheidend, Fehlverhalten kann zu großen materiellen und immateriellen Schäden mit teilweise beträchtlichen negativen Kundeneffekten führen.

Im Folgenden für dich im Überblick wichtige Kernaussagen aus der DSGVO und dem BDSG:

Unterschied Datenschutz und Datensicherheit: Der Datenschutz schützt nicht die Daten – der Begriff ist insofern nicht korrekt. Vielmehr geht es um den Schutz der Menschen davor, nicht über Gebühr von Dritten „verdatet“ zu werden. Hintergrund sind die Persönlichkeitsrechte, aufgrund derer Daten, die sich auf eine Person beziehen, immer auch dieser zugeordnet werden können und diese in gewisser Weise „abbilden“. Dafür gibt es Grenzen, die regeln, wie sehr man eine Person „verdaten“ darf – dies sind die Datenschutzgesetze.

Die Datensicherheit dagegen kümmert sich rein um die Daten selbst und um deren technischen, aber auch organisatorischen Schutz, etwa durch Verschlüsselung, einem Rollen- und Berechtigungskonzept, etc.

Personenbezogene Daten (Art. 4 Nr. 1 DSGVO): Der Datenschutz betrifft nur personenbezogene Daten. Dies sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen, wie zum Beispiel Mitarbeiter, Kollegen, Kunden, Lieferanten, etc. Dazu zählen z. B. Adresse, Telefonnummer, Geburtsdatum, Foto, Gehalt, Urlaubsplanung, Arbeitsverhalten, Arbeitsergebnisse. Auch Daten ohne direkten Personenbezug (z. B. ohne Namensangabe) können personenbezogene Daten sein, wenn aus ihnen die zugehörige Person zumindest identifizierbar ist (z. B. Personalnummer, PC-Benutzerkennung, etc.). 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.

Verbotsprinzip und Zweckbindung (Art. 5, 6 DSGVO): Die Verarbeitung personenbezogener Daten ist nach dem Datenschutzrecht grundsätzlich verboten, wenn nicht ausnahmsweise per Gesetz die geplante Datenverarbeitung erlaubt ist oder der Betroffene darin eingewilligt hat. Vor einer Datenverarbeitung ist also zu prüfen, ob eine solche Ausnahme gegeben ist, ebenso wie, ob alle damit einhergehenden gesetzlichen Begleitpflichten eingehalten werden, wie die Informationspflichten.

Grundsätzlich dürfen Daten nur für den Zweck, für den sie erhoben wurden, auch verarbeitet werden; jede Zweckänderung muss erlaubt sein.

Aufteilung eines Gesamtvorgangs: Wenn eine Datenverarbeitung aus mehreren Teilschritten besteht (Dateneingabe, Datenweitergabe, Nutzung der Daten für Zweck 1, für Zweck 2, etc.) muss jeder Einzelschritt für sich genommen betrachtet und nach einer möglichen Verarbeitungserlaubnis und etwaigen Begleitpflichten geprüft werden. So gelten regelmäßig

* Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

für das Speichern von Daten andere Vorgaben als für deren Auswertungen.

Sog. „sensitive“/ „sensible“ Daten (Art. 9 DSGVO): Bestimmte Arten personenbezogener Daten (oft als sensitive oder sensible Daten bezeichnet) dürfen in aller Regel nur auf Basis einer Einwilligung des Betroffenen erhoben und verarbeitet werden. Darunter fallen Angaben über rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, das Sexualleben oder strafrechtliche Verurteilungen. Auch ansonsten gelten für diese Daten oft besondere Vorschriften. Nur in wenigen Sonderfällen besteht für die Verarbeitung dieser Daten eine Erlaubnis per Gesetz.

Rechte der Betroffenen (Art. 12 ff. DSGVO): Jeder, dessen personenbezogene Daten verarbeitet werden, hat gegenüber der verantwortlichen Stelle verschiedene Rechte, wie das Recht auf Auskunft u. a. über gespeicherte Daten, Zweck der Speicherung sowie Herkunft und Empfänger von Übermittlungen. Unzutreffende Daten muss die verantwortliche Stelle berichtigen, unzulässig gespeicherte oder nicht mehr erforderliche Daten zu löschen. Wenn jemandem durch eine unrechtmäßige automatisierte Verarbeitung seiner personenbezogenen Daten ein Schaden zugefügt wird, ist ihm Schadenersatz zu gewähren.

Datensicherheit durch technische und organisatorische Maßnahmen (Art. 25, 32 DSGVO): Das Gesetz verlangt die Umsetzung von angemessenen technischen und organisatorischen Maßnahmen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Dabei ist vorgegeben, dass die Technik, mit der personenbezogene Daten verarbeitet werden, schon von Beginn an möglichst so gestaltet ist, dass die Datenschutzgrundsätze wirksam umgesetzt werden („privacy by design“). Dies umfasst auch die Pflicht, die Technik wie auch Geschäftsprozesse schon von Anfang an so zu gestalten und „voreinzustellen“, dass die Vorgaben eingehalten werden („privacy by default“).

Meldeprozesse bei Verstößen (Art. 33 DSGVO): Im Fall der Verletzung des Schutzes personenbezogener Daten können für uns als Unternehmen sehr strenge Meldepflichten gegenüber den Behörden gelten. Es ist daher äußerst wichtig, dass jeder Mitarbeiter, der von einer solchen Datenschutzverletzung erfährt, diese sofort dem Datenschutz-Manager und / oder dem Datenschutzbeauftragten meldet, damit dort geprüft werden kann, was die nächsten Schritte sind. Achtung: Wir haben dazu in Form einer Datenschutz-Richtlinie einen festen Prozess definiert, der einzuhalten ist. Diese Richtlinie findest du im Intranet oder erhältst sie von unserem Datenschutz-Management.

Jeder einzelne Mitarbeiter ist für die Einhaltung der Datenschutzvorgaben verantwortlich. Richtiges Verhalten ist daher unabdingbar.

Bei Fragen zum Thema Datenschutz bzw. Datensicherheit oder in Zweifelsfällen wende dich bitte – lieber einmal zu oft als zu wenig – an datenschutz@bavaria-film.de.

* Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Anlage 2 zur Verpflichtung auf die Vertraulichkeit

Auswahl gesetzlicher Vorschriften aus DSGVO und BDSG

Die vorliegende Auswahl gesetzlicher Vorschriften soll dir einen Überblick über das datenschutzrechtliche Regelwerk verschaffen. Die Darstellung erfolgt exemplarisch und ist keineswegs vollständig. Weitere Informationen zu datenschutzrechtlichen Fragestellungen erhältst du bei unserem Datenschutzbeauftragten.

Begrifflichkeiten

Art. 4 Nr. 1 DSGVO: „**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 DSGVO: „**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.

Grundsätze der Verarbeitung

Art. 5 Abs. 1 lit. a DSGVO: 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 DSGVO: 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 DSGVO: 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 DSGVO: 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.

* Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Art. 33 Abs. 1 Satz 1 DSGVO: 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.

Haftung und Strafen

Art. 82 Abs. 1 DSGVO: 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 DSGVO: 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 machtund 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 erschleichtund 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.

* Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Fernmeldegeheimnis (soweit für dich relevant)

§ 3 TTDSG

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

(2) Zur Wahrung des Fernmeldegeheimnisses sind verpflichtet

1. Anbieter von öffentlich zugänglichen Telekommunikationsdiensten sowie natürliche und juristische Personen, die an der Erbringung solcher 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.

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.

* Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.