Verpflichtung zur Vertraulichkeit nach DSGVO für freie Mitarbeiter

Als Unternehmen sind wir gesetzlich verpflichtet, personenbezogene Daten so zu verarbeiten, dass die Rechte der durch die Verarbeitung betroffenen Personen auf Vertraulichkeit und Integrität ihrer Daten gewährleistet werden[1]. Daher dürfen Sie personenbezogene Daten nur in dem Umfang und in der Weise verarbeiten, wie es zur Erfüllung der Ihnen übertragenen Aufgaben erforderlich ist.

Nach diesen Vorschriften dürfen Sie personenbezogene Daten nicht unbefugt oder unrechtmäßig verarbeiten oder absichtlich oder unabsichtlich die Sicherheit der Verarbeitung in einer Weise verletzen, die zur Vernichtung, zum Verlust, zur Veränderung, zur unbefugten Offenlegung oder unbefugtem Zugang führt.

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 arbeitsvertragliche Pflichten dar, der entsprechend geahndet werden kann.

Die Verpflichtung auf die Vertraulichkeit besteht auch nach der Beendigung des Auftragsverhältnisses fort.

_____[*Name des freien Mitarbeiters*] erklärt gegenüber _____

_____[*Name der beauftragenden Burda Gesellschaft*], in Bezug auf die Vertraulichkeit und Integrität personenbezogener Daten die Vorgaben der geltenden Datenschutzvorschriften einzuhalten.

Mit Ihrer Unterschrift bestätigen Sie zugleich den Empfang einer Kopie dieser Niederschrift nebst Anlagen.

_____, _____ _____

Ort Datum Unterschrift Verpflichtete(r)

Anlagen:

1. Überblick über die wesentlichen Datenschutzrechtlichen Bestimmungen
2. Technische und organisatorische Maßnahmen

[1] Sollte Ihre Tätigkeit das Fernmeldegeheimnis, das Sozialgeheimnis, oder die anwaltliche oder ärztliche Schweigepflicht berühren, gelten über die Datenschutzgrundverordnung und die übrigen allgemeinen datenschutzrechtlichen Bestimmungen hinaus weitere gesetzliche Vorgaben, die Sie bei Ihrer Tätigkeit zu beachten haben.

Überblick über die wesentlichen datenschutzrechtlichen Bestimmungen

Anlage 1 zur Verpflichtung zur Vertraulichkeit für freie Mitarbeiter

Die vorliegende Auswahl gesetzlicher Vorschriften soll Ihnen als Überblick über die wichtigsten datenschutzrechtlichen Bestimmungen dienen. Die Darstellung erfolgt exemplarisch und ist keineswegs vollständig. Weitere Informationen zu datenschutzrechtlichen Fragestellungen erhalten Sie beim betrieblichen Datenschutzbeauftragten.

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.

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.

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.

Technische und organisatorische Maßnahmen

Anlage 2 zur Verpflichtung zur Vertraulichkeit für freie Mitarbeiter

Hubert Burda Media („**HBM**“) ergreift geeignete technische und organisatorische Maßnahmen, um den Schutz personenbezogener Daten und die Vertraulichkeit von Informationen sicherzustellen. Je sensibler die Daten sind, auf die der freie Mitarbeiter[1] Zugriff erhält, desto sorgfältiger sind diese zu schützen. Hierbei gelten die folgenden Rahmenbedingungen:

1. Nutzung von HBM IT-Systemen

Bei der Nutzung von IT-Systemen von HBM, sind:

a) keine Änderungen an den Sicherheitseinstellungen vorzunehmen;
b) ausschließlich Hard- und Software zu nutzen, die vorab von der Abteilung iSecurity und von HBM Datenschutz freigegeben wurde (z.B. Apps);
c) nur USB-Sticks zu verwenden, die von HBM zur Verfügung gestellt wurden (die Verwendung von USB-Festplatten ist nicht gestattet);
d) keine Cloud-Dienste zu nutzen, die nicht von dem Information Security Officer („**ISO**“) der beauftragenden HBM-Gesellschaft oder dem Chief Information Security Officer („**CISO**“) von HBM freigegeben wurden;
e) keine Inhalte anzubieten oder abzurufen, die gegen datenschutz-, persönlichkeits-, urheber- oder strafrechtliche Bestimmungen verstoßen;
f) Inhalte in digitaler Form nur in Abstimmung mit dem internen Ansprechpartner bei HBM öffentlich zu verbreiten (z.B. Newsletter);
g) IT-Systeme und Daten mit einem sicheren Passwort vor dem Zugriff Dritter zu schützen und dieses Passwort nicht weiterzugeben;
h) beruflich genutzte Accounts von Anbietern wie Apple, Amazon oder Google, von einer zentralen Stelle im Unternehmen verwalten zu lassen;
i) private Accounts nicht für dienstliche Zwecke zu verwenden; keine privaten Accounts in den bereitgestellten E-Mail-Programmen (z.B. Outlook) zu erstellen;
j) ausschließlich von HBM bereitgestellte Cloud-Dienste für die Ablage von HBM-Daten zu verwenden;
k) interne Anwendungen auf mobilen IT-Systemen ausschließlich über besonders gesicherte Netzwerkverbindungen zu verwenden;
l) bei Beendigung der Zusammenarbeit persönliche Daten zu löschen, Unternehmensdaten (inkl. Passwörter auch für externe Dienste, die beruflich genutzt wurden) nach Absprache dem jeweiligen Ansprechpartner bei HBM zu übergeben bzw. zu löschen.

2. Nutzung eigener IT-Systeme

Wenn der freie Mitarbeiter eigene IT-Systeme nutzt, muss er gegenüber dem ISO der beauftragenden HBM-Gesellschaft oder dem CISO geeignete technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten und der Vertraulichkeit von Informationen für den konkreten Einzelfall nachweisen können, die einen gleichwertigen Schutz wie die unter Ziff. 1 aufgeführten Maßnahmen bieten.

[1] Im Folgenden wird jeweils die männliche Form einer Personenbezeichnung verwendet. Sämtliche Personenbezeichnungen gelten gleichwohl für beiderlei Geschlecht.