Gesellschaft für Datenschutz
und Datensicherheit e.V.

GDD-Praxishilfe DS-GVO XI

Verpflichtung auf die Vertraulichkeit

INHALT

Verpflichtung auf die Vertraulichkeit

Das bisherige Datenschutzrecht sah eine sog. „Verpflichtung auf das Datengeheimnis“ vor. § 5 BDSG a.F. lautete: „Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.“

Eine vergleichbar klare und eindeutige Regelung ist in der DS-GVO nicht mehr enthalten. Insoweit stellt sich datenverarbeitenden Unternehmen die Frage, ob die klassische Verpflichtung auf das Datengeheimnis weiterhin eine Zukunft hat. Falls eine derartige förmliche Verpflichtung der Mitarbeiter notwendig bleibt, könnte ggf. ein Update der Alt-Verpflichtungen notwendig sein.

Die vorliegende Praxishilfe soll einen Überblick über das Wesen und den Inhalt einer Verpflichtungserklärung gewähren. Ein entsprechendes Muster ist beigefügt.

1. Verpflichtung auf die Vertraulichkeit

1.1 Verpflichtung als valide organisatorische Maßnahme

Der Akt der Verpflichtung ist mehr als nur ein Ritual[1]. Er besitzt eine deutliche **Warn- und Belehrungsfunktion**. Im Rahmen der Dokumentations- und Nachweispflichten des Art. 5 Abs. 2 DS-GVO (Accountability) ist die Verpflichtung der zur Verarbeitung befugten Personen auch weiterhin als probates Mittel anzusehen, um die Einhaltung datenschutzrechtlicher Vorschriften von vornherein zu gewährleisten.

> **Zu den Rechenschaftspflichten nach Art. 5 Abs. 2 DS-GVO siehe GDD-Praxishilfe DS-GVO IX – Accountability.**

Dies zeigt sich unter anderem am Regime der Auftragsverarbeitung (AV), welches in Art. 28 Abs. 3 lit. b DS-GVO die Verpflichtung auf die Vertraulichkeit zumindest beim Dienstleister ausdrücklich als Pflichtinhalt des AV-Vertrages vorsieht.

Darüber hinaus legt Art. 32 Abs. 4 DS-GVO fest, dass sowohl Verantwortliche als auch Auftragsverarbeiter Schritte zu unternehmen haben, um sicherzustellen, dass die unterstellten Personen mit Zugang zu personenbezogenen Daten nur auf Anweisung des Verantwortlichen tätig werden. Art. 29 DS-GVO bezieht sich ebenfalls auf diese eindeutig weisungsabhängige Verarbeitung. Hierzu gehört es, unmissverständlich auf die Bedeutung und den Umfang datenschutzrechtlicher Regeln hinzuweisen und Mitarbeitern etwaige Risiken von Gesetzesverstößen vor Augen zu führen.

Der Bundesgesetzgeber hat im Rahmen der Umsetzung der Richtlinie 2016/680/EU für den Datenschutz in Polizei und Justiz an der förmlichen Verpflichtung festgehalten. § 53 BDSG n.F. verwendet insoweit sogar den hergebrachten Begriff des Datengeheimnisses. Was im öffentlichen Bereich recht ist, kann daher im nicht-öffentlichen Bereich nur billig sein.

Bei berufs- und standesrechtlicher Verschwiegenheitspflicht ist das Weglassen einer Verpflichtung für mitwirkende Personen gem. § 203 Abs. 4 Satz 2 Nr. 1 StGB ggf. sogar strafbewehrt, falls die mitwirkende Person unbefugt fremde Geheimnisse offenbart.

1.2 Inhalt und Folgen

Die Verpflichtung auf die Vertraulichkeit verweist unmittelbar auf Art. 5 Abs. 1 lit. f DS-GVO („Integrität und Vertraulichkeit“) und damit auf

- angemessene **Sicherheit** der personenbezogenen Daten;
- Schutz vor **unbefugter oder unrechtmäßiger Verarbeitung**;
- Schutz vor unbeabsichtigtem **Verlust**;
- Schutz vor unbeabsichtigter **Zerstörung** oder unbeabsichtigter **Schädigung**.

Flankiert wird diese Regelung durch Art. 32 Abs. 2 DS-GVO, wonach unter anderem

1 Ehmann, ZD 2017, 453

- die **unbefugte Offenlegung** sowie
- der **unbefugte Zugang** zu personenbezogenen Daten

unterbunden werden soll.

Entsprechende Erklärungen können auch im bereichsspezifischen Datenschutzrecht sinnvoll sein, falls etwa das **Fernmeldegeheimnis** (vgl. § 88 TKG), das **Sozialgeheimnis** (z.B. kraft Verweisung in § 78 Abs. 1 Satz 3 SGB X n.F.) oder **Berufsgeheimnisse** (vgl. § 203 StGB) einschlägig sein sollten.

Die Verpflichtung wirkt derweil nicht konstitutiv, d.h. die gesetzlichen Vorgaben des Datenschutzrechts gelten auch ohne individuelle Vergatterung. Anders ist dies lediglich bei einer Verpflichtung nach dem Verpflichtungsgesetz (VerpflG), welche eine eigenständige strafbewehrte Geheimnisträgereigenschaft gem. § 203 Abs. 2 Nr. 2 StGB begründet. Die rein deklaratorische Verpflichtung auf die Vertraulichkeit z.B. nach der DS-GVO oder dem TKG ist hiermit nicht identisch.

1.3 Form und Zeitpunkt

Da die DS-GVO zur Verpflichtung weitestgehend schweigt, ist keine bestimmte Form vorgesehen. Es bietet sich jedoch im Beweisinteresse an, die **Schriftform nebst eigenhändiger Unterschrift** zu wählen. Es ist auch denkbar, die Verpflichtung am Ende eines eLearning-Prozesses oder im Rahmen eines digitalen Belehrungsprozesses vorzunehmen und zu dokumentieren.

Die Verpflichtung erfüllt nur dann ihren Zweck, wenn sie vor Aufnahme der datenverarbeitenden Tätigkeit erfolgt. Bei der Aufnahme eines Arbeits- oder Dienstverhältnisses kann die Verpflichtung zusammen mit den Vertragsunterlagen abgezeichnet werden, es sollte jedoch darauf geachtet werden, dass die Erklärung nicht in einer Fülle von Unterlagen verschwindet. Insoweit ist zumindest ein gesondertes Dokument – mit Abdruck der entscheidenden Gesetzespassagen zum Verbleib beim Mitarbeiter – anzuraten. Die Aushändigung eines allgemeinen Merkblatts oder der Unternehmens-Policy zum Datenschutz kann hilfreich sein.

Das Muster einer Unternehmensrichtlinie zur Datenschutz-Organisation finden Sie in der GDD-Praxishilfe DS-GVO VIII.

1.4 Fortgeltung von Alt-Verpflichtungen

Einer **Neuverpflichtung** auf die Vertraulichkeit am 25. Mai 2018 bedarf es nicht[2]. Sie würde insbesondere bei einer großen Zahl von Beschäftigten in unnötigen Formalismus ausufern. Gerade weil die Verpflichtung nicht konstitutiv wirkt, sondern lediglich eine Warn- und Belehrungsfunktion besitzt, vermögen vorangegangene Erklärungen nach bisherigem Recht diese ebenso gut zu erfüllen.

Im Rahmen der Schulung und Beratung sämtlicher Mitarbeiter im Sinne von Art. 39 Abs. 1 lit. a DS-GVO ist es jedoch sinnvoll, auf die Änderungen im Datenschutzrecht in geeigneter Form, ggf. per Rundschreiben hinzuweisen.

2 Franck, ZD 2017, 509, 513

2. Muster

Das nachfolgende Muster soll in der gebotenen Knappheit über die allgemeinen Datenschutzgrundsätze informieren. Die Verpflichtungserklärung selbst nimmt keinen unmittelbaren Bezug auf einzelne Rechtsnormen. Hierdurch wird die Lesbarkeit erhöht. Eine exemplarische Auswahl an einschlägigen Rechtsvorschriften findet sich stattdessen in der beigefügten Anlage. Die Verpflichtung alleine kann unterdessen keine umfassende Schulung ersetzen.

Verpflichtung auf die Vertraulichkeit

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 Ihnen auch nur gestattet, personenbezogene Daten in dem Umfang und in der Weise zu verarbeiten, wie es zur Erfüllung der Ihnen übertragenen Aufgaben 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 unbefugter 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.

Optional – Ihre Tätigkeit berührt das Fernmeldegeheimnis. Sie dürfen sich nicht über das erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation verschaffen. Sie dürfen derartige Kenntnisse grundsätzlich nicht an Dritte weitergeben.

Optional – Ihre Tätigkeit berührt das Sozialgeheimnis. Sofern Daten verarbeitet werden, die dem Sozialgeheimnis unterliegen, haben Sie diese im gleichen Umfang geheim zu halten, wie die ursprünglich übermittelnde Stelle.

Optional – Ihre Tätigkeit berührt die [anwaltliche/ärztliche/etc.] Schweigepflicht. Sie wirken an der beruflichen oder dienstlichen Tätigkeit eines Berufsgeheimnisträgers mit, soweit dies erforderlich ist. Es ist Ihnen untersagt, fremde Geheimnisse, namentlich zum persönlichen Lebensbereich gehörende Geheimnisse oder Betriebs- oder Geschäftsgeheimnisse unbefugt zu offenbaren.

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

Frau/Herr _____ Abteilung/Tätigkeit _____

erklärt, 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 Anlage.

_____, _____ _____

Ort, Datum Verpflichtete(r)

Anlage zur Verpflichtung auf die Vertraulichkeit

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

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.

Optional – Fernmeldegeheimnis

§ 88 TKG

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

(2) [1]Zur Wahrung desFernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. [2]Die Pflicht zur Geheimhaltung besteht **auch nach dem Ende der Tätigkeit** fort, durch die sie begründet worden ist.

(3) [1]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 Umständen der Telekommunikation zu verschaffen. [2]Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den in Satz 1 genannten Zweck verwenden. [3]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. [4]Die Anzeigepflicht nach § 138 des Strafgesetzbuches hat Vorrang. [...]

Optional – Sozialgeheimnis

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

Optional – Berufsgeheimnis

§ 203 StGB

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die

Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,

2. Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlußprüfung,

3. Rechtsanwalt, Kammerrechtsbeistand, Patentanwalt, Notar, Verteidiger in einem gesetzlich geordneten Verfahren, Wirtschaftsprüfer, vereidigtem Buchprüfer, Steuerberater, Steuerbevollmächtigten oder Organ oder Mitglied eines Organs einer Rechtsanwalts-, Patentanwalts-, Wirtschaftsprüfungs-, Buchprüfungs- oder Steuerberatungsgesellschaft,

4. Ehe-, Familien-, Erziehungs- oder Jugendberater sowie Berater für Suchtfragen in einer Beratungsstelle, die von einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts anerkannt ist,

5. Mitglied oder Beauftragten einer anerkannten Beratungsstelle nach den §§ 3 und 8 des Schwangerschaftskonfliktgesetzes,

6. staatlich anerkanntem Sozialarbeiter oder staatlich anerkanntem Sozialpädagogen oder
7. Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen, steuerberaterlichen oder anwaltlichen Verrechnungsstelle

anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft. […]

(4) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer unbefugt ein fremdes Geheimnis offenbart, das ihm bei der Ausübung oder bei Gelegenheit seiner Tätigkeit als **mitwirkende Person** oder als bei den in den Absätzen 1 und 2 genannten Personen tätiger Beauftragter für den Datenschutz bekannt geworden ist. […]

Gesellschaft für Datenschutz
und Datensicherheit e.V.

Die Inhalte dieser Praxishilfe wurden im Rahmen des GDD-Arbeitskreises „DS-GVO Praxis“ erstellt.

Satz: C. Wengenroth, GDD-Geschäftsstelle, Bonn

Herausgeber:
Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.)
Heinrich-Böll-Ring 10
53119 Bonn
Tel.: +49 2 28 96 96 75-00
Fax: +49 2 28 96 96 75-25
www.gdd.de
info@gdd.de

Stand:
Version 1.1 (Dezember 2017)