Gesellschaft für Datenschutz
und Datensicherheit e.V.

GDD-Praxishilfe DS-GVO IV

Vertragsmuster zur Auftragsverarbeitung

INHALT

1. Vorwort 3

2. Auftragsverarbeitung nach BDSG und DS-GVO

(Synopse 2013 / 2017)

GDD-MUSTER 2013 (Muster: Auftrag gemäß § 11 BDSG) ..... 4 – 20

GDD-MUSTER 2017 (Muster: Auftragsverarbeitung gemäß Art. 28 DS-GVO) ..... 4 – 20

3. Technisch-organisatorische Maßnahmen ..... 21 – 22

Vertragsmuster zur Auftragsverarbeitung

Zur Anpassung der Datenschutzorganisation an die neuen Anforderungen der DS-GVO gehört unter anderem die Überprüfung bestehender Vertragsverhältnisse sowie die Anpassung der Vertragsmuster für zukünftige Outsourcing-Dienstleistungen.[1] Für den Bereich der Auftragsverarbeitung sind viele Einzelfragen noch in der Diskussion, sei es die Abgrenzung zur Funktionsübertragung oder zur gemeinsamen Verantwortlichkeit, das Fortbestehen der bisherigen Privilegierung von Auftragsverhältnissen oder schlicht die Anwendung auf Fernwartungsvorgänge. Diese Fragen müssen durch Wissenschaft und Praxis und insbesondere den noch zu konstituierenden Europäischen Datenschutzausschuss befriedigend gelöst werden.

Unterarbeitsgruppen zur Auftragsverarbeitung bestehen derzeit in den GDD-Erfa-Kreisen Hannover, Köln und Nürnberg sowie dem GDD-Arbeitskreis Datenschutz im Gesundheits- und Sozialwesen.

In der vorliegenden Praxishilfe werden zunächst die GDD-Vertragsmuster von 2013 (§ 11 BDSG) und 2017 (Art. 28 DS-GVO) gegenübergestellt. Die Pflichtinhalte nach alter und künftiger Rechtslage sind dabei bemerkenswert deckungsgleich. Im Idealfall sollten Altverhältnisse auf das neue Muster umgestellt werden, da dieses spezifisch auf die gesetzlichen Erfordernisse der DS-GVO abgestimmt wurde. Sofern stattdessen am alten Vertrag festgehalten werden muss, bedarf es geringfügiger Nachbesserungen, um die gesetzlichen Mindestanforderungen zu erfüllen.

Freilich soll nicht unterschlagen werden, dass ein Vertragswerk zur Auftragsverarbeitung nicht allein von den gesetzlichen Pflichtinhalten lebt. Geeignete fakultative Regelungen runden das neue Muster ab und sorgen für einen angemessenen Interessenausgleich zwischen den Vertragsparteien.

---

1 Siehe auch GDD-Praxishilfe DS-GVO III „To-Dos für die Übergangsfrist bis zur Geltung der DS-GVO“, Punkt 3.5.

Auftragsverarbeitung nach BDSG und DS-GVO

GDD-MUSTER 2013 A

Muster: Auftrag gemäß § 11 BDSG

Vereinbarung

zwischen dem/der

_____

- nachstehend Auftraggeber genannt -
und dem/der

_____

- nachstehend Auftragnehmer genannt -

Hinweis auf Seite 1:
„Die einzelnen schriftlichen Festlegungen nach § 11 Abs. 2 Nr. 1 bis Nr. 10 BDSG sollten vollständig in die Vereinbarung übernommen und wie eine Checkliste abgearbeitet werden. Die für das konkrete Dienstleistungsverhältnis zutreffenden Alternativen sollten angekreuzt werden. Leerfelder sind ggf. entsprechend des konkreten Auftrags auszufüllen."

1. Gegenstand und Dauer des Auftrags

Gegenstand des Auftrags

☐ Der Gegenstand des Auftrags ergibt sich aus der Leistungsvereinbarung/SLA/_____ _____ vom _____, auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung).

oder

*(weiter unter **Grau B, C, D** usw.)*

GDD-MUSTER 2017 A

Muster: Auftragsverarbeitung gemäß Art. 28 DS-GVO

Vereinbarung

zwischen dem/der

_____

- Verantwortlicher -
nachstehend Auftraggeber genannt - und dem/der

_____

ggf.: Vertreter gemäß Art. 27 DS-GVO:

_____

- Auftragsverarbeiter -
nachstehend Auftragnehmer genannt

Hinweis:
„Die einzelnen Festlegungen nach Art. 28 Abs. 3 DS-GVO sollten vollständig in die Vereinbarung übernommen und wie eine Checkliste abgearbeitet werden. Die für das konkrete Dienstleistungsverhältnis zutreffenden Alternativen sollten angekreuzt werden. Leerfelder sind ggf. entsprechend des konkreten Auftrags auszufüllen. Vergütungs- und Haftungsregelungen zu den einzelnen Leistungen des Auftragnehmers sollten im Hauptvertrag vereinbart werden."

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

☐ Der Gegenstand des Auftrags ergibt sich aus der Leistungsvereinbarung/SLA/_____ _____ vom _____, auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung).

oder

*(weiter unter **Rot B, C, D** usw.)*

GDD-MUSTER 2013 B

Muster: Auftrag gemäß § 11 BDSG

☐ Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

_____

(Definition der Aufgaben)

Dauer des Auftrags

☐ Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

oder *(insbesondere, falls keine Leistungsvereinbarung zur Dauer besteht)*

☐ Der Auftrag wird zur einmaligen Ausführung erteilt.

oder

☐ Die Dauer dieses Auftrags (Laufzeit) ist befristet bis zum _____

oder

☐ Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von _____ zum _____ gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

> Ziffer 1 des Vertrages entspricht Art. 28 Abs. 3 S. 1 DS-GVO.

2. Konkretisierung des Auftragsinhalts:

Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten

☐ Umfang, Art und Zweck der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung vom _____

oder

GDD-MUSTER 2017 B

Muster: Auftragsverarbeitung gemäß Art. 28 DS-GVO

☐ Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

_____

(Definition der Aufgaben)

(2) Dauer

☐ Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

oder *(insbesondere, falls keine Leistungsvereinbarung zur Dauer besteht)*

☐ Der Auftrag wird zur einmaligen Ausführung erteilt.

oder

☐ Die Dauer dieses Auftrags (Laufzeit) ist befristet bis zum _____

oder

☐ Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von _____ zum _____ gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

2. Konkretisierung des Auftragsinhalts:

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

☐ Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung vom _____

oder

GDD-MUSTER 2013 C

Muster: Auftrag gemäß § 11 BDSG

☐ Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Umfang, Art und Zweck der Aufgaben des Auftragnehmers: _____

Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der §§ 4b, 4c BDSG erfüllt sind.

GDD-MUSTER 2017 C

Muster: Auftragsverarbeitung gemäß Art. 28 DS-GVO

☐ Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers: _____

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

> **i** Eine Beschränkung auf die Bundesrepublik ist mit Blick auf das nunmehr EU-weit einheitliche Datenschutzniveau nicht mehr angezeigt.

Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind. Das angemessene Schutzniveau in _____

☐ ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO);

☐ wird hergestellt durch verbindliche interne Datenschutzvorschriften (Artt. 46 Abs. 2 lit. b iVm 47 DS-GVO);

☐ wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und d DS-GVO);

☐ wird hergestellt durch genehmigte Verhaltensregeln (Artt 46 Abs. 2 lit. e iVm 40 DS-GVO);

☐ wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Artt. 46 Abs. 2 lit. f i.V.m. 42 DS-GVO).

GDD-MUSTER 2013 D

Muster: Auftrag gemäß § 11 BDSG

Art der Daten

☐ Die Art der verwendeten personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben unter: _____

oder

☐ Gegenstand der Erhebung, Verarbeitung und/ oder Nutzung personenbezogener Daten sind folgende Datenarten/ -kategorien (Aufzählung/ Beschreibung der Datenkategorien)

- ☐ Personenstammdaten
- ☐ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Kundenhistorie
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Planungs- und Steuerungsdaten
- ☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

Kreis der Betroffenen

☐ Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen ist in der Leistungsvereinbarung konkret beschrieben unter: _____

oder

GDD-MUSTER 2017 D

Muster: Auftragsverarbeitung gemäß Art. 28 DS-GVO

☐ wird hergestellt durch sonstige Maßnahmen:

_____

(Art. 46 Abs 2 lit. a, Abs. 3 litt. a und b DS-GVO)

Bei beabsichtigten Drittlandstransfers sind insbesondere die Ziffern 5 lit. c (Vertreter in der Union) und 6 Abs. 4 (Unterauftragnehmer im Drittland) des Vertragsmusters zu berücksichtigen.

(2) Art der Daten

☐ Die Art der verwendeten personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben unter:_____

oder

☐ Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- ☐ Personenstammdaten
- ☐ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Kundenhistorie
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Planungs- und Steuerungsdaten
- ☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- ☐ ...

3) Kategorien betroffener Personen

☐ Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der Leistungsvereinbarung konkret beschrieben unter:_____

oder

GDD-MUSTER 2013 E

Muster: Auftrag gemäß § 11 BDSG

☐ Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen umfasst (Aufzählung/Beschreibung der betroffenen Personenkategorien):
☐ Kunden
☐ Interessenten
☐ Abonnenten
☐ Beschäftigte i. S. d. § 3 Abs. 11 BDSG
☐ Lieferanten
☐ Handelsvertreter
☐ Ansprechpartner
☐ ...

Ziffer 2 des Vertrages entspricht Art. 28 Abs. 3 S. 1 DS-GVO. Dass sich die Herstellung des angemessenen Datenschutzniveaus im Drittland künftig nicht mehr nach den §§ 4b, 4c BDSG sondern nach den Artt. 44 ff. DS-GVO bestimmt, ist unschädlich und im Rahmen der Vertragsauslegung zu berücksichtigen.

3. Technisch-organisatorische Maßnahmen

Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

GDD-MUSTER 2017 E

Muster: Auftragsverarbeitung gemäß Art. 28 DS-GVO

☐ Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:
☐ Kunden
☐ Interessenten
☐ Abonnenten
☐ Beschäftigte
☐ Lieferanten
☐ Handelsvertreter
☐ Ansprechpartner
☐ ...

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

GDD-MUSTER 2013 F

Muster: Auftrag gemäß § 11 BDSG

Insgesamt handelt es sich bei den zu treffenden Maßnahmen um nicht auftragsspezifische Maßnahmen hinsichtlich der Organisationskontrolle, Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle sowie des Trennungsgebots (vgl. Anlage ...), sowie andererseits um auftragsspezifische Maßnahmen, insbesondere im Hinblick auf die Art des Datenaustauschs/Bereitstellung von Daten, Art/Umstände der Verarbeitung/der Datenhaltung sowie Art/Umstände beim Output/Datenversand, die – soweit sie sich nicht aus der zugrundeliegenden Leistungsvereinbarung ergeben - wie folgt gesondert beschrieben werden:

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren. Der Auftragnehmer hat auf Anforderung die Angaben nach § 4g Abs. 2 Satz 1 BDSG dem Auftraggeber zur Verfügung zu stellen.

Ziffer 3 des Vertrages entspricht Art. 28 Abs. 3 S. 2 lit. c DS-GVO. Dass sich die Bewertungsgrundlage von § 9 BDSG auf Art. 32 DS-GVO verschiebt, ist unschädlich und im Rahmen der Vertragsauslegung zu berücksichtigen.

GDD-MUSTER 2017 F

Muster: Auftragsverarbeitung gemäß Art. 28 DS-GVO

(2) Der Auftragnehmer hat die Sicherheit gem. Artt. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

GDD-MUSTER 2013 G

Muster: Auftrag gemäß § 11 BDSG

4. Berichtigung, Sperrung und Löschung von Daten

„Der Auftragnehmer hat nur nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten."

Ziffer 4 des Vertrages entspricht in Teilen Art. 28 Abs. 3 S. 2 lit. e DS-GVO. Der Verweis auf die Organisationskontrolle in Ziffer 3 fängt etwaige Verkürzungen im Hinblick auf die künftigen Betroffenenrechte auf.

5. Kontrollen und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags nach § 11 Abs. 4 BDSG folgende Pflichten:

>> Schriftliche Bestellung – soweit gesetzlich vorgeschrieben – eines Datenschutzbeauftragten, der seine Tätigkeit gemäß §§ 4f, 4g BDSG ausüben kann. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt.

GDD-MUSTER 2017 G

Muster: Auftragsverarbeitung gemäß Art. 28 DS-GVO

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

Der Auftraggeber kann vertraglich zur Übernahme der anfallenden Mehrkosten verpflichtet werden.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) ☐ Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausübt.

☐ Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

GDD-MUSTER 2013 H

Muster: Auftrag gemäß § 11 BDSG

>> Die Wahrung des Datengeheimnisses entsprechend § 5 BDSG. Alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, müssen auf das Datengeheimnis verpflichtet und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt werden.

Die Klausel entspricht Art. 28 Abs. 3 S. 2 lit. b DS-GVO.

GDD-MUSTER 2017 H

Muster: Auftragsverarbeitung gemäß Art. 28 DS-GVO

☐ Als Datenschutzbeauftragte(r) ist beim Auftragnehmer Herr/Frau [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail] bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

☐ Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

b) ☐ Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Herr/Frau [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail] benannt.

c) ☐ Da der Auftragnehmer seinen Sitz außerhalb der Union hat, benennt er folgenden Vertreter nach Art. 27 Abs. 1 DS-GVO in der Union: [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail].

d) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

Eine gesetzliche Verpflichtung zur Verarbeitung kann z.B. bei Herausgabeverlangen von Ermittlungsbehörden bestehen.

GDD-MUSTER 2013

Muster: Auftrag gemäß § 11 BDSG

>> Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechend § 9 BDSG und Anlage.

Die Klausel entspricht Art. 28 Abs. 3 S. 2 lit. c DS-GVO. Dass sich die Bewertungsgrundlage von § 9 BDSG auf Art. 32 DS-GVO verschiebt, ist unschädlich und im Rahmen der Vertragsauslegung zu berücksichtigen.

>> Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde nach § 38 BDSG. Dies gilt auch, soweit eine zuständige Behörde nach §§ 43, 44 BDSG beim Auftragnehmer ermittelt.

GDD-MUSTER 2017

Muster: Auftragsverarbeitung gemäß Art. 28 DS-GVO

e) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].

f) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

g) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

h) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

Der Auftraggeber kann vertraglich zur Übernahme der anfallenden Mehrkosten verpflichtet werden. Der Auftragnehmer kann wegen fehlender Kostenübernahme durch den Auftraggeber jedoch kein Leistungsverweigerungsrecht gegenüber der Behörde geltend machen.

GDD-MUSTER 2013 J

Muster: Auftrag gemäß § 11 BDSG

>> Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den Auftragnehmer im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags.

Die Klausel entspricht Art. 28 Abs. 3 S. 2 lit. h DS-GVO.

>> Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber. Hierzu kann der Auftragnehmer auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) vorlegen.

Die Klausel entspricht Art. 28 Abs. 3 S. 2 litt. c und h DS-GVO.

GDD-MUSTER 2017 J

Muster: Auftragsverarbeitung gemäß Art. 28 DS-GVO

i) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

Zum sog. PDCA-Zyklus („plan-do-check-act“) siehe GDD-Praxishilfe DS-GVO II „Verantwortlichkeiten und Zuständigkeiten nach der DS-GVO“, Punk 2.1.

j) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

Soweit bei der Verarbeitung oder Nutzung personenbezogener Daten des Auftraggebers Unterauftragnehmer einbezogen werden sollen, wird dies genehmigt, wenn folgende Voraussetzungen vorliegen:

>> Die Einschaltung von Unterauftragnehmern ist grundsätzlich nur mit schriftlicher Zustimmung des Auftraggebers gestattet. Ohne schriftliche Zustimmung kann der Auftragnehmer zur Vertragsdurchführung unter Wahrung seiner unter Punkt 5 erläuterten Pflicht zur Auftragskontrolle konzernangehörige Unternehmen sowie im Einzelfall andere Unterauftragnehmer mit der gesetzlich gebotenen Sorgfalt einsetzen, wenn er dies dem Auftraggeber vor Beginn der Verarbeitung oder Nutzung mitteilt.

>> Der Auftragnehmer hat die vertraglichen Vereinbarungen mit dem/den Unterauftragnehmer/n so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen.

>> Bei der Unterbeauftragung sind dem Auftraggeber Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung und des § 11 BDSG i.V.m. Nr. 6 der Anlage zu § 9 BDSG beim Unterauftragnehmer einzuräumen. Dies umfasst auch das Recht des Auftraggebers, vom Auftragnehmer auf schriftliche Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.

Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftrags-

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

a) ☐ Eine Unterbeauftragung ist unzulässig.

b) ☐ Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

Firma Unterauftragnehmer	Anschrift / Land	Leistung

durchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

Die Klausel entspricht Art. 28 Abs. 2, Abs. 3 S. 2 lit. d, Abs. 4 DS-GVO.

c) ☐ Die Auslagerung auf Unterauftragnehmer oder
☐ der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:
>> der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und

Ggf. ist die Vereinbarung einer Meldefrist (bspw. 2 Wochen) sowie eine Festlegung einer Frist vor dem Zeitpunkt der Übergabe der Daten ratsam.

>> der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
>> eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

GDD-MUSTER 2013 M

Muster: Auftrag gemäß § 11 BDSG

7. Kontrollrechte des Auftraggebers

Der Auftraggeber hat das Recht, die in Nr. 6 der Anlage zu § 9 BDSG vorgesehene Auftragskontrolle im Benehmen mit dem Auftragnehmer durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen.

Im Hinblick auf die Kontrollverpflichtungen des Auftraggebers nach § 11 Abs. 2 S. 4 BDSG vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragnehmer dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß § 9 BDSG und der Anlage nach. Dabei kann der Nachweis der Umsetzung

GDD-MUSTER 2017 M

Muster: Auftragsverarbeitung gemäß Art. 28 DS-GVO

(5) Eine weitere Auslagerung durch den Unterauftragnehmer

☐ ist nicht gestattet;

☐ bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);

☐ bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform);

sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

☐ die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;

☐ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;

☐ aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer,

solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, auch durch Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden.

Die Klausel entspricht Art. 28 Abs. 3 S. 1, S. 2 lit. h DS-GVO.

8. Mitteilung bei Verstößen des Auftragnehmers

Der Auftragnehmer erstattet in allen Fällen dem Auftraggeber eine Meldung, wenn durch ihn oder die bei ihm beschäftigten Personen Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind.

Es ist bekannt, dass nach § 42a BDSG Informationspflichten im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten bestehen können. Deshalb sind solche Vorfälle ohne Ansehen der Verursachung unverzüglich dem Auftraggeber mitzuteilen. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers. Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen. Soweit den Auftraggeber

Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

☐ eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informa-

GDD-MUSTER 2013 0

Muster: Auftrag gemäß § 11 BDSG

Pflichten nach § 42a BDSG treffen, hat der Auftragnehmer ihn hierbei zu unterstützen.

Die Klausel entspricht zum Teil Art. 28 Abs. 3 S. 2 lit. f DS-GVO. Der Verweis auf § 42a BDSG ist unschädlich, da bereits in der Eingangsformel sämtliche Verstöße gegen Vorschriften zum Schutz personenbezogener Daten genannt sind. Der Maßstab verschiebt sich nunmehr in Richtung Artt. 33 f. DS-GVO, was bei der Vertragsauslegung zu berücksichtigen ist.

Eine gesetzliche Verpflichtung zur Verarbeitung kann z.B. bei Herausgabeverlangen von Ermittlungsbehörden bestehen.

9. Weisungsbefugnis des Auftraggebers

Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers (vgl. § 11 Abs. 3 Satz 1 BDSG). Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

GDD-MUSTER 2017 0

Muster: Auftragsverarbeitung gemäß Art. 28 DS-GVO

tionen unverzüglich zur Verfügung zu stellen

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

Auf welche Weise der Auftragnehmer den Auftraggeber unterstützt, ist von der Art der Dienstleistung abhängig. Entsprechende Maßnahmen sollten vertraglich konkretisiert werden.

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

Die Ziffer 9 wurde im neuen Muster erheblich verschlankt. Die allgemeinen Regeln zur Weisungsbefugnis finden sich bereits in Ziffer 5 lit. d (Qualitätssicherung) des Musters. Ziffer 9 ist Besonderheiten vorbehalten.

GDD-MUSTER 2013 P

Muster: Auftrag gemäß § 11 BDSG

Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

Die Klauseln entsprechend Art. 28 Abs. 3 S. 2 lit. a DS-GVO.

Der Auftragnehmer hat den Auftraggeber unverzüglich entsprechend § 11 Abs. 3 Satz 2 BDSG zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

Die Klausel entspricht Art. 28 Abs. 3 UAbs. 2 DS-GVO.

GDD-MUSTER 2017 P

Muster: Auftragsverarbeitung gemäß Art. 28 DS-GVO

weiter auf Seite 20

GDD-MUSTER 2013

Muster: Auftrag gemäß § 11 BDSG

10. Löschung von Daten und Rückgabe von Datenträgern

Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Die Klausel entspricht Art. 28 Abs. 3 S. 2 lit. g DS-GVO.

GDD-MUSTER 2017

Muster: Auftragsverarbeitung gemäß Art. 28 DS-GVO

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Anlage
Technisch-organisatorische Maßnahmen

Auch die technisch-organisatorischen Maßnahmen werden mit der DS-GVO grundüberholt. Die bekannten Pflichten aus § 9 BDSG nebst Anlage behalten grundsätzlich ihre Gültigkeit, sie werden der Systematik des Art. 32 Abs. 1 DS-GVO unterworfen. Die Zuordnung ist dabei lediglich redaktioneller Natur. So vermag etwa das Trennungsprinzip sowohl Aspekte der Vertraulichkeit, der Integrität als auch der Belastbarkeit zu fördern.

Neu hinzu tritt die obligatorische Einführung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung. Darüber hinaus wird künftig die Pseudonymisierung als eigenständige Maßnahme im Verordnungstext genannt.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;

>> **Zugangskontrolle**

Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;

>> **Zugriffskontrolle**

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;

>> **Trennungskontrolle**

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;

>> **Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)**

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

>> **Weitergabekontrolle**

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;

>> **Eingabekontrolle**

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

>> **Verfügbarkeitskontrolle**

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

>> **Datenschutz-Management;**
>> **Incident-Response-Management;**
>> **Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);**
>> **Auftragskontrolle**
Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

Alle zu treffenden Maßnahmen sind vertraglich konkret zu bestimmen - pauschale Aussagen und Wiederholungen der gesetzlichen Vorschriften genügen hierfür nicht. Das BayLDA hat in einem Fall unzureichender Regelung bereits ein Bußgeld in fünfstelliger Höhe festgesetzt (https://www.lda.bayern.de/media/pm2015_11.pdf).

Gesellschaft für Datenschutz
und Datensicherheit e.V.

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

Mit freundlicher Unterstützung durch die Unterarbeitsgruppen „Auftragsverarbeitung“ der GDD-Erfa-Kreise Köln und Nürnberg.

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 (April 2017)