Gesellschaft für Datenschutz
und Datensicherheit e.V.

GDD-Praxishilfe DS-GVO IV

Mustervertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

INHALT

Mustervertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

Nachdem die gesetzlichen Mindestanforderungen an den Vertrag zur Auftragsverarbeitung (AV) in der EU-Datenschutzrichtlinie nur rudimentär ausgestaltet waren, sieht die DS-GVO nunmehr weitreichende Anforderungen an den Vertrag mit dem Auftragsverarbeiter vor.

Während die erste Auflage dieser Praxishilfe eine Gegenüberstellung zwischen alter und neuer Rechtslage beinhaltete, findet sich in der Aktualisierung nunmehr ein einheitliches Vertragsmuster. Sie enthält, neben der bewährten, rundum aktualisierten AV-Mustervorlage, nunmehr Erläuterungen zu den einzelnen Vertragsklauseln und wird durch allgemeine Hinweise zur Erleichterung der Abgrenzung zwischen Verantwortlichem und Auftragsverarbeiter ergänzt. Als Grundlage für die Überarbeitung der Vertragsklauseln dienten u.a. Vertragsmuster von offizieller Seite, insbesondere seitens der Aufsichtsbehörden für den Datenschutz auf nationaler und europäischer Ebene.

Da ein Vertragswerk zur Auftragsverarbeitung nicht allein von den gesetzlichen Pflichtinhalten lebt, runden geeignete fakultative (optionale) Regelungen das neue Muster ab und sorgen für einen angemessenen Interessenausgleich zwischen den Vertragsparteien.

1. Gesetzliche Definitionen

Im Sinne der DS-GVO bezeichnet der Ausdruck:
„Verantwortlicher" die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden (Art. 4 Nr. 7 DS-GVO).

„Auftragsverarbeiter" eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (Art. 4 Nr. 8 DS-GVO).

2. Abgrenzung zwischen Auftragsverarbeitung und Verantwortlichkeit

Art. 28 DS-GVO regelt die Anforderungen an die Auftragsverarbeitung, einschließlich der Anforderungen an den Vertrag und die Verarbeitung personenbezogener Daten durch weitere Auftragsverarbeiter (Unterauftragnehmer), ohne auf die Frage einzugehen, wann eine Auftragsverarbeitung in Abgrenzung zu einer Übermittlung an einen Verantwortlichen oder an gemeinsam für die Verarbeitung Verantwortliche überhaupt vorliegt. Auch die gesetzliche Definition des Auftragsverarbeiters hilft hier nur bedingt weiter, da sie lediglich von einem "Auftrag" spricht, der durch eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle ausgeführt wird, wobei personenbezogene Daten verarbeitet werden.

Entscheidendes Kriterium für die Abgrenzung zwischen einem datenschutzrechtlich Verantwortlichen und einem Auftragsverarbeiter (Art. 28 DS-GVO) ist die Weisungsgebundenheit des Auftragsverarbeiters im Verhältnis zum Auftraggeber. Während der Verantwortliche einen **steuernden und kontrollierenden Einfluss** auf die Zwecke oder wesentlichen Mittel der Verarbeitung nimmt[1], unterwirft sich der Auftragsverarbeiter insofern den Weisungen des Verantwortlichen und wird lediglich als dessen „verlängerter Arm" tätig. Der Auftragnehmer entscheidet nach Auffassung des Europäischen Datenschutzausschusses dementsprechend nur über sog. **"nicht essenzielle Mittel"**, so z.B. über die für den jeweiligen Datenverarbeitungsprozess einzusetzende Hard- und Software oder über spezifische Sicherheitsmaßnahmen.[2] Denkbar sind jedoch auch organisatorische Aspekte, beispielsweise die Organisation des Personaleinsatzes, die ein Auftragsverarbeiter ohne explizite Weisung des Auftraggebers steuert.

Der Inanspruchnahme von Dienstleistungen ist immanent, dass die Detailkenntnisse über die Verarbeitungsprozesse häufig beim Dienstleister liegen und diesem vielfach ein Entscheidungsspielraum eingeräumt ist, mit welchen Mitteln er die vom Verantwortlichen bestimmten Zwecke erreicht. Expertise und überlegenes Wissen allein führen nicht zur Verantwortlichkeit, solange die **Entscheidung über die Zwecke und wesentlichen Mittel der Verarbeitung** beim Auftraggeber verbleibt. Einer Auftragsverarbeitung steht auch nicht entgegen, dass das Konzept für die Datenverarbeitung inklusive der Zwecke und wesentlichen Mittel der Verarbeitung vom Dienstleister entwickelt wurde, solange der Auftraggeber das Konzept akzeptiert und der Dienstleister im Folgenden nur weisungsgebunden agiert.

Indiz für eine Auftragsverarbeitung kann sein, wenn ein Akteur über den Verarbeitungsprozess hinaus **keine eigenen Interessen** an den Daten oder an dem Ergebnis hat, welches aus der Verarbeitung resultiert. Der Auftragsverarbeiter benötigt zur Legitimation der Verarbeitung lediglich einen Vertrag

1 Vgl. HK/Kremer, DS-GVO/BDSG, 2018, Art. 26 Rn. 22.
2 European Data Protection Board (EDPB), Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 1.0 (version for public consultation), Nr. 38.

mit dem Verantwortlichen. Letzterer hat die datenschutzrechtliche Verantwortung gegenüber der betroffenen Person und benötigt stets eine eigene Rechtsgrundlage für die Verarbeitung.[3]

Klassische Anwendungsbereiche für die Auftragsverarbeitung sind etwa die Auslagerung der Lohn- und Gehaltsabrechnung, Archivierungsvorgänge und Konvertierungen von Dokumenten, Verarbeitungen von Kundendaten durch Call-Center ohne wesentliche eigene Entscheidungsspielräume oder die Datenträgerentsorgung. Praxisbeispiele für eine Auftragsverarbeitung nach Art. 28 DS-GVO sind auch der Hostprovider und Software as a Service (SaaS) Angebote, sofern der SaaS-Dienstleister die Daten nicht z.B. auch für eigene Auswertungen zu Zwecken der Qualitätssicherung oder Produktoptimierung verwendet.[4]

Kontrovers diskutiert wird weiterhin das Vorliegen einer Auftragsverarbeitung im Rahmen der **Prüfung und Wartung von IT-Systemen**. Die Datenschutzkonferenz geht davon aus, dass im Falle einer Beauftragung von Fehleranalysen oder Support-Arbeiten in Systemen des Auftraggebers und einer damit einhergehenden Möglichkeit des Zugriffs auf personenbezogene Daten es sich um eine Form oder Teiltätigkeit der Auftragsverarbeitung gem. Art. 28 DS-GVO handele.[5] Der Europäische Datenschutzausschuss stellt bei der vorzunehmenden Abgrenzung zum einen darauf ab, ob der Auftragnehmer mit der Verarbeitung personenbezogener Daten überhaupt beauftragt wird. Erfolge bspw. die Beauftragung eines Auftragnehmers lediglich mit der Fehleranalyse innerhalb einer Software und würden personenbezogene Daten dabei allenfalls **beiläufig und in begrenztem Umfang** zur Kenntnis genommen werden, wäre die Implementierung angemessener technisch-organisatorischer Maßnahmen gem. Art. 32 DS-GVO zum Schutz der personenbezogenen Daten als ausreichend anzusehen. Auf eine Auftragsverarbeitung könne daher verzichtet werden.[6] Im Falle des allgemeinen IT-Supports als Auftrag für den Auftragnehmer und einer unvermeidbaren, systematischen Zugriffsmöglichkeit auf personenbezogene Daten, sei der Abschluss eines Vertrages zur Auftragsverarbeitung hingegen erforderlich.[7]

Aus praktischer Sicht ist es für Verantwortliche ratsam, sich mit der Frage der Beauftragung einer Verarbeitung *personenbezogener Daten* auseinander zu setzen. Ergeben sich aus dem Auftrag unweigerlich Zugriffsmöglichkeiten auf Systeme und Applikationen mit personenbezogenen Daten, wird der Abschluss eines Vertrages zur Auftragsverarbeitung zu empfehlen sein. Lediglich bei Einzelbeauftragungen, bei denen Zugriffsmöglichkeiten auf personenbezogene Daten weitestgehend auszuschließen ist, können rein technisch-organisatorische Maßnahmen gegenüber dem Auftragnehmer erwogen werden.

3. Grundlage der Verarbeitung

Art. 28 Abs. 3 S. 1 DS-GVO fordert, dass die Verarbeitung durch einen Auftragsverarbeiter auf der Grundlage eines Vertrags erfolgt, der den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet. Alternativ kann die Auftragsverarbeitung auch auf Basis eines anderen Rechtsinstruments nach

3 GDD-Praxishilfe XV: Die gemeinsame Verantwortlichkeit nach Art. 26 DS-GVO (Joint Controllership), S. 23 ff. Dort findet sich auch eine Checkliste als Hilfestellung zur Abgrenzung der Auftragsverarbeitung und alleiniger/ gemeinsamer Verantwortlichkeit (vgl. Ziff. 9.2. ff).
4 Weitere Beispiele finden sich im FAQ des Bayerischen Landesamts für Datenschutzaufsicht "Abgrenzung Auftragsverarbeitung", vgl. https://www.lda.bayern.de/media/FAQ_Abgrenzung_Auftragsverarbeitung.pdf.
5 Vgl. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz), Kurzpapier Nr. 13, S. 3.
6 European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Nr. 81 („IT-consultant fixing a software bug").
7 European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Nr. 81 ("General IT-Support").

dem Unionsrecht oder dem Recht der Mitgliedstaaten ihre Grundlage haben. Dies kann die Erteilung des Auftrags durch Verordnung, Richtlinie oder formelles Gesetz sein[8] und findet bspw. im Bereich der Datenverarbeitung im Auftrag von öffentlichen Stellen Anwendung, wo ein Vertragsschluss ungewöhnlich ist.[9] Art. 28 Abs. 3 S. 1 Hs. 2 und S. 2 DS-GVO befassen sich im Weiteren mit den **Mindestinhalten**[10] des Vertrags oder anderen Rechtsinstruments. Ferner werden in der Praxis – neben besonderen Anforderungen des Verantwortlichen oder Auftragsverarbeiters - vertragliche Regelungen zu den Vorgaben des Art. 28 Abs. 2 u. 4 DS-GVO an die Verarbeitung personenbezogener Daten durch weitere Auftragsverarbeiter im Vertrag zur Auftragsverarbeitung zu finden sein.

Die gesetzlich geforderte **Form** des Vertragsschlusses ist in Art. 28 Abs. 9 DS-GVO geregelt. Hiernach ist der Vertrag oder das andere Rechtsinstrument schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann. Dies kann grundsätzlich **jede Verkörperung des Erklärungsinhalts** auf einem beliebigen Erklärungsträger sein. Die elektronische Form i.S.d § 126a BGB, die eine qualifizierte elektronische Signatur voraussetzt, muss hierbei nicht eingehalten werden.[11] Allerdings muss nachvollziehbar sein, dass die Vertragsparteien, die in dem Dokument genannt sind, sich tatsächlich zu den eingegangenen Verpflichtungen mit dem konkreten Inhalt bekannt haben. Dies ist bei der Auswahl eines elektronischen Formats[12] zu berücksichtigen, so dass bspw. der Austausch einer einfachen E-Mail ohne elektronische Signierung regelmäßig nicht ausreichend sein dürfte.[13]

4. Vertragsmuster

Das nachfolgende Muster stellt ein allgemeines Muster zur Auftragsverarbeitung dar und ist im Einzelfall an die Bedürfnisse der Vertragsparteien anzupassen. Die hochgestellten Ordnungszahlen stellen Verweise zu den erläuternden Hinweisen am Ende dieser Praxishilfe dar. Die einzelnen Festlegungen nach Art. 28 Abs. 3 DS-GVO sollten im Übrigen 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.

8 Ehmann/Selmayr/Bertermann Art. 28 Rn. 13
9 Gola DS-GVO/Klug DS-GVO Art. 28 Rn. 7.
10 Vgl. Art. 28 Abs. 3 S. 2 DS-GVO: Dieser Vertrag bzw. dieses andere Rechtsinstrument sieht insbesondere vor, .[…]
11 Vgl. Paal/Pauly/Martini, DS-GVO BDSG Art. 28, Rn. 75 m.w.N.
12 Näher hierzu vgl. LDA Bayern, FAQ zur DS-GVO, abrufbar unter https://www.lda.bayern.de/media/FAQ_ADV_Formerfordernis.pdf sowie Stellungnahme der EU-Kommission abrufbar unter http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2018-003163&language=EN.
13 S. auch Müthlein, RDV 2016, 74 (76), der vom Erfordernis einer einfachen Signatur ausgeht.

Vertrag

zwischen dem/der

.....
- Verantwortlicher -
nachstehend Auftraggeber genannt -

und dem/der

.....
- Auftragsverarbeiter -
nachstehend Auftragnehmer genannt -

1. Gegenstand und Dauer des Vertrags[1]

(1) Gegenstand

❑ Der Gegenstand des Vertrags ergibt sich aus der Leistungsvereinbarung/dem SLA/dem Auftrag ..... vom ....., auf die/den/das hier verwiesen wird (im Folgenden Leistungsvereinbarung).

oder

❑ Gegenstand des Vertrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: ..... (Beschreibung der Aufgaben)

(2) Dauer

❑ Die Dauer dieses Vertrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.
oder (insbesondere, falls keine Leistungsvereinbarung zur Dauer besteht)

❑ Der Vertrag beinhaltet eine einmalige Ausführung.

oder

❑ Die Dauer dieses Vertrags (Laufzeit) ist befristet bis zum .....

oder

❑ Der Vertrag wird für unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist von ..... zum ..... gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

(3) Der Vertrag gilt unbeschadet des vorstehenden Absatzes so lange, wie der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet (einschließlich Backups).

(4) Soweit sich aus anderen Vereinbarungen zwischen Auftraggeber und Auftragnehmer anderweitige Abreden zum Schutz personenbezogener Daten ergeben, soll dieser Vertrag zur Auftragsverarbeitung vorrangig gelten, es sei denn die Parteien vereinbaren ausdrücklich etwas anderes.

2. Konkretisierung des Vertragsinhalts[2]

(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

❑ Nähere Beschreibung des Vertragsgegenstandes im Hinblick auf Art und Zweck der Aufgabe des Auftragnehmers: .....

(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

❑ Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ❑ Kunden
- ❑ Interessenten
- ❑ Abonnenten
- ❑ Beschäftigte
- ❑ Lieferanten
- ❑ Handelsvertreter
- ❑ Ansprechpartner
- ❑ ...

3. Technisch-organisatorische Maßnahmen[3]

(1) Der Auftragnehmer ergreift in seinem Verantwortungsbereich alle erforderlichen technisch-organisatorische Maßnahmen gem. Art. 32 DS-GVO zum Schutz der personenbezogenen Daten und übergibt dem Auftraggeber die Dokumentation zur Prüfung [Anlage 1]. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Vertrags.

(2) Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(3) Die vereinbarten technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer zukünftig gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Über wesentliche Änderungen, die durch den Auftragnehmer zu dokumentieren sind, ist der Auftraggeber unverzüglich in Kenntnis zu setzten.

[OPTIONALE KLAUSEL] Die Verarbeitung von Daten, die diesem Vertrag unterliegen, ist in Privatwohnungen nicht gestattet (Heim- und Telearbeit).

4. Rechte von betroffenen Personen[4]

(1) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich mittels geeigneter technisch-organisatorischer Maßnahmen bei der Beantwortung und Umsetzung von Anträgen betroffener Personen hinsichtlich ihrer Datenschutzrechte. Er darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers beauskunften, portieren, 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 die Rechte auf Auskunft, Berichtigung, Einschränkung der Verarbeitung, Löschung sowie Datenportabilität nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

(1) Der Auftragnehmer hat, zusätzlich zu der Einhaltung der Regelungen dieses Vertrags, eigene gesetzliche Pflichten gemäß der DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Die Wahrung der Vertraulichkeit[5] 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 berechtigterweise 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.

b) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen[6].

c) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde[7], soweit sie sich auf diesen Vertrag 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.

d) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten, einem anderen Anspruch oder einem Informationsersuchen im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen[8].

e) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen[9], 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.

f) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen[10] gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 8 dieses Vertrags.

g) Der Auftragnehmer meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber in der Weise, dass der Auftraggeber seinen gesetzlichen Pflichten, insbesondere nach Artt. 33, 34 DS-GVO nachkommen kann[11]. Er fertigt über den gesamten Vorgang eine Dokumentation an, die er dem Auftraggeber für weitere Maßnahmen zur Verfügung stellt.

h) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich im Rahmen bestehender Informationspflichten gegenüber Aufsichtsbehörden und Betroffenen und stellt ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zu Verfügung.

i) Soweit der Auftraggeber zur Durchführung einer Datenschutz-Folgenabschätzung verpflichtet ist, unterstützt ihn der Auftragnehmer unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen. Gleiches gilt für eine etwaig bestehende Pflicht zur Konsultation der zuständigen Datenschutz-Aufsichtsbehörde.

(2) Dieser Vertrag entbindet den Auftragnehmer nicht von der Einhaltung anderer Vorgaben der DS-GVO.

6. Unterauftragsverhältnisse[12]

(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 in Anspruch nimmt, z.B. Telekommunikationsleistungen, Post-/ Transportdienstleistungen, Reinigungsleistungen oder Bewachungsdienstleistungen. Wartungs- und Prüfleistungen stellen dann ein Unterauftragsverhältnis dar, wenn sie für IT-Systeme erbracht werden, die im Zusammenhang mit einer Leistung des Auftragnehmers nach diesem Vertrag erbracht werden. 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 zu treffen 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 in Anhang 2 bezeichneten Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO mit dem Unterauftragnehmer zu.

Die vertragliche Vereinbarung wird dem Auftraggeber auf dessen Verlangen vorgelegt, wobei geschäftliche Klauseln ohne datenschutzrechtlichen Bezug hiervon ausgenommen sind.

c) ❑ Die Auslagerung auf Unterauftragnehmer oder
❑ der Wechsel der gemäß Anhang 2 bestehenden Unterauftragnehmer sind zulässig, soweit:
> der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber in einer angemessenen Zeit, die 14 Tage nicht unterschreiten darf, vorab schriftlich oder in Textform anzeigt und
> 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. Die Einhaltung und Umsetzung der technisch-organisatorischen Maßnahmen beim Unterauftragnehmer wird unter Berücksichtigung des Risikos beim Unterauftragnehmer vorab der Verarbeitung personenbezogener Daten und sodann regelmäßig durch den Auftragnehmer kontrolliert. Der Auftragnehmer stellt dem Auftraggeber die Kontrollergebnisse auf Anfrage zur Verfügung. Der Auftragnehmer stellt ferner sicher, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Kontrollrechte) auch direkt gegenüber den Unterauftragnehmern wahrnehmen kann.

(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.

(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. Internationale Datentransfers[13]

(1) Jede Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation bedarf einer dokumentierten Weisung des Auftraggebers und bedarf der Einhaltung der Vorgaben zur Übermittlung personenbezogener Daten in Drittländer nach Kapitel V der DS-GVO.

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

❑ Der Auftraggeber gestattet eine Datenübermittlung in ein Drittland. In der Anlage 2 werden die Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus aus Art. 44 ff. DS-GVO im Rahmen der Unterbeauftragung spezifiziert.

(2) Soweit der Auftraggeber eine Datenübermittlung an Dritte in ein Drittland anweist, ist er für die Einhaltung von Kapitel V der DS-GVO verantwortlich.

8. Kontrollrechte des Auftraggebers[14]

(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 während der üblichen Geschäftszeiten 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 der technisch-organisatorischen Maßnahmen zur Einhaltung der besonderen Anforderungen des Datenschutzes allgemein sowie solche, die den 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, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
❑ eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

9. Weisungsbefugnis des Auftraggebers[15]

(1) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf Basis dokumentierter Weisungen des Auftraggebers, es sei denn er ist nach dem Recht des Mitgliedstaats oder nach Unionsrecht zu einer Verarbeitung verpflichtet. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform). Die anfänglichen Weisungen des Auftraggebers werden durch diesen Vertrag festgelegt.

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften[16]. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten[17]

(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 aber 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.

Anlage I

Technisch-organisatorische Maßnahmen

Beschreibung der technisch-organisatorischen Maßnahmen des Auftragnehmers unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten betroffener Personen.

Soweit einschlägig,

[Beschreibung von Maßnahmen der Pseudonymisierung und Verschlüsselung personenbezogener Daten]

[Beschreibung von Maßnahmen zur Gewährleistung einer kontinuierlichen Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung]

[Beschreibung von Maßnahmen zur Gewährleistung der Verfügbarkeit personenbezogener Daten und des raschen Zugangs zu Daten im Falle eines physischen oder technischen Zwischenfalls]

[Beschreibung von Maßnahmen zur Gewährleistung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung]

[Beschreibung von Maßnahmen zur Identifizierung und Authentifizierung von Nutzern]

[Beschreibung von Maßnahmen zum Schutz personenbezogener Daten bei der Übertragung]

[Beschreibung von Maßnahmen zum Schutz personenbezogener Daten bei ihrer Speicherung]

[Beschreibung von Maßnahmen zur Gewährleistung einer physischen Sicherheit von Orten, an denen personenbezogene Daten verarbeitet werden]

[Beschreibung von Maßnahmen zum Schutz personenbezogener Daten bei der Heim- oder Telearbeit]*

[Beschreibung von Anforderungen an die Ereignisprotokollierung (z.B. bei der Nutzerauthentifizierung oder der Dateneingabe, -veränderung oder -löschung]

[Beschreibung technisch-organisatorischer Maßnahmen im Rahmen der Unterstützungspflichten des Auftragnehmers (z.B. bei den Betroffenenrechten)]

---

* Nicht zu beschreiben, wenn die Heim- und Telearbeit gem. der optionalen Klausel aus Ziff. 3 des Vertragsmusters untersagt wurde.

Anlage II

Genehmigte Unterauftragsverhältnisse

Firma Unterauftragnehmer	Anschrift/Land	Leistung	Angaben zu geeigneten Garantien bei Daten-übermittlungen in ein Drittland

5. Kommentare zu den Vertragsklauseln

1. Gegenstand und Dauer des Vertrags. Art. 28 Abs. 3 S. 1 DS-GVO sieht vor, dass Gegenstand und Dauer der Verarbeitung personenbezogener Daten zwischen Auftraggeber und Auftragnehmer festgelegt werden. Ein Verweis bspw. auf eine Leistungsvereinbarung oder ein SLA sind dann möglich, wenn dort eine hinreichend konkrete Beschreibung des Gegenstandes sowie der Dauer der Verarbeitung erfolgt.

2. Konkretisierung des Vertragsinhalts. Ausweislich der gesetzlichen Vorgabe müssen Art und Zweck der Verarbeitung personenbezogener Daten spezifiziert werden. Solche Darstellungen werden in Leistungsvereinbarungen oder SLAs in der Praxis seltener zu finden sein, so dass hier regelmäßig ergänzender Dokumentationsbedarf besteht.

Die Beschreibung von Kategorien betroffener Personen kann anhand der Darstellung von Zusammenfassungen von Betroffenen nach bestimmten Merkmalen, so bspw. Kunden oder Beschäftigte, erfolgen. Hinsichtlich der Datenarten bietet es sich an, Angaben hierzu auf Datenverwendungen zu beschränken, die auch explizit Gegenstand des Auftrags sind. Beiläufig anfallende Daten (z.B. Protokolldateien) sind hiervon regelmäßig nicht erfasst.

3. Technisch-organisatorische Maßnahmen. Der Auftraggeber soll nur mit solchen Auftragsverarbeitern zusammenarbeiten, die mittels geeigneter technischer und organisatorischer Maßnahmen eine Datenverarbeitung im Einklang mit der Grundverordnung sowie zum Schutz der Rechte der Betroffenen gewährleisten können (Art. 28 Abs. 1 DS-GVO). Insofern, und gesetzlich explizit von ihm gefordert, muss der Auftragsverarbeiter alle erforderlichen Maßnahmen gem. Art. 32 DS-GVO ergreifen und dies gegenüber dem Auftraggeber vertraglich bestätigen (vgl. Art. 28 Abs. 3 S. 2 lit. c DS-GVO). Die getroffenen technisch-organisatorischen Maßnahmen müssen die IT-Schutzziele der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit adressieren. Eine abstrakte Zusicherung reicht nicht aus, da der Verantwortliche sich auf Basis abstrakter Beschreibung kein ausreichendes Bild über die Datensicherheit beim Auftragnehmer machen kann. Insofern verweist das Vertragsmuster auf Maßnahmen des Art. 32 DS-GVO, die durch den Auftragnehmer hinsichtlich ihrer Umsetzung zu konkretisieren sind. Gesetzliche Schutzziele, die für die Dienstleistung nicht relevant sind, müssen nicht beschrieben werden. Ob eine Dokumentation bzw. Konkretisierung der technisch-organisatorischen Maßnahmen über eine Anlage zum Vertrag oder bspw. durch Zusendung eines IT-Sicherheitskonzepts erfolgt, liegt im Ermessen der Parteien. Die Beschreibungen des Auftragnehmers müssen den Auftraggeber in die Lage versetzen, seiner Kontrollpflicht auftragsbezogen effektiv nachzukommen. Der Auftraggeber hat die vorgelegten Dokumente hinsichtlich Prüfgegenstand, Prüftiefe Vollständigkeit und Übereinstimmung mit dem konkreten Auftrag zu überprüfen.

Soweit der Auftraggeber nach Prüfung der technisch-organisatorischen Maßnahmen einen Anpassungsbedarf erkennt, wird er diesen einvernehmlich mit dem Auftragnehmer umsetzen. Hierdurch werden die gem. Art. 32 DS-GVO standardmäßig angebotenen Maßnahmen des Auftragnehmers modifiziert, was einvernehmlich zu erfolgen hat.

Dem Auftragnehmer ist es gestattet, seine technisch-organisatorischen Maßnahmen weiterzuentwickeln und zu ändern. Das mit dem Auftraggeber festgelegte Schutzniveau zum Vertragsschluss darf jedoch hierbei nicht unterschritten werden. Besagte Weiterentwicklungen vollziehen sich regelmäßig ohne die gesonderte Genehmigung durch den Auftraggeber, da sie sich nach diesem Vertragsmuster auf die eigenen, standardmäßig angebotenen technisch-organisatorischen Maßnahmen gem. Art. 32 DS-GVO beziehen. Nichtsdestotrotz ist der Auftraggeber über solche Änderungen zu informieren, um über das aktuelle Schutzniveau beim Auftragnehmer im Bilde zu sein.

4. Rechte von Betroffenen. Als verlängerter Arm des Verantwortlichen sowie als weisungsgebundener Datenverarbeiter steht es dem Auftragnehmer grundsätzlich nicht zu, eigenmächtig über eine Datenverarbeitung zu entscheiden. Daher ist es ihm auch untersagt, ohne entsprechende Weisung des Auftraggebers, Anfragen von Betroffenen, so u.a. über die zu seiner/ihrer Person gespeicherten Daten oder auf Löschung von Daten oder deren Berichtigung, zu beantworten. Es ist jedoch möglich, bestimmte Verarbeitungen, die eigentlich im Verantwortungsbereich des Verantwortlichen stehen, vertraglich auf den Auftragnehmer zu delegieren.
Ferner ist zu empfehlen, die Unterstützungsleistungen des Auftragnehmers bei den Rechten von Betroffenen im Rahmen der technisch-organisatorischen Maßnahmen zu konkretisieren, so bspw. im Rahmen der Auskunftsersuchen von Betroffenen.

5. Wahrung der Vertraulichkeit. Gem. Art. 28 Abs. 3 S. 2 lit. b DS-GVO verpflichtet sich der Auftragnehmer, Mitarbeiter, die auf personenbezogene Daten des Auftraggebers zur Auftragserfüllung zugreifen dürfen, zur Vertraulichkeit zu verpflichten. Die GDD hat über die Praxishilfe XI ein entsprechendes Muster hierzu veröffentlicht.

Je nach Auftragsverhältnis bietet es sich an, besondere Regelungen zur Zulässigkeit des mobilen Arbeitens oder der Telearbeit durch Mitarbeiter des Auftragnehmers im Vertrag zu treffen (z.B. das Verbot der Heim- oder Telearbeit der ein Zustimmungserfordernis auf Seiten des Auftraggebers). Ebenfalls bietet es sich an, Angaben zur Gewährleistung der Vertraulichkeit hierbei in der Vertragsanlage zu den technisch-organisatorischen Maßnahmen zu dokumentieren.

6. Zusammenarbeit mit der Aufsichtsbehörde. In Art. 31 DS-GVO findet sich die Vorgabe, dass Verantwortliche und Auftragsverarbeiter sowie ggf. deren Vertreter auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammenarbeiten. Im Auftragsverarbeitungsverhältnis bietet es sich an, dies vertraglich zu fixieren, damit beide Parteien im Falle einer aufsichtsbehördlichen Anfrage die notwendige Unterstützung des Vertragspartners erhalten.

7. Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde. Art. 28 Abs. 1 DS-GVO statuiert, dass der Auftraggeber nur mit Auftragsverarbeitern zusammenarbeitet, die mittels geeigneter technisch-organisatorischer Maßnahmen für eine Verarbeitung im Einklang mit der DS-GVO sorgen und den Schutz der Rechte von Betroffenen gewährleisten. Eine Kontrollhandlung oder sonstige Maßnahme beim Auftragnehmer, sei es bspw. im Rahmen eines Straf- oder Ordnungswidrigkeitenverfahrens, kann ein Indiz dafür sein, dass entsprechende Schutzmaßnahmen beim Auftragsverarbeiter nicht gewährleistet sind. Daher sieht das Vertragsmuster eine entsprechende Information des Auftraggebers im Falle solcher Kontrollhandlungen vor. Besagte Information soll jedoch nur für auftragsrelevante Handlungen und Maßnahmen gelten, zumal der Auftragnehmer auch Verarbeitungen zu eigenen Zwecken regelmäßig durchführt (z.B. im Rahmen der Verarbeitung von Daten seiner Beschäftigten).

8. Unterstützung des Auftraggebers. Art. 28 Abs. 3 lit. e u. f DS-GVO sieht Unterstützungspflichten des Auftragsverarbeiters explizit im Rahmen der Beantwortung von Anträgen zur Wahrnehmung von Betroffenenrechten nach Kapitel III, sowie bei der Einhaltung der Pflichten nach Artt. 32 bis 36 DS-GVO vor. Das Vertragsmuster erweitert diese Unterstützungspflichten auf die im Vertragsmuster genannten Sachverhalte, da es hier ebenfalls notwendig sein kann, dass der Auftraggeber auf Informationen oder Maßnahmen des Auftragnehmers angewiesen ist. Andernfalls entstünden Haftungsrisiken auf Seiten des Auftraggebers, wenn er auf eine Mitwirkung des Auftragnehmers angewiesen ist, er jedoch über keine vertraglichen Durchsetzungsmöglichkeiten diesbezüglich verfügt.

Den Vertragsparteien ist es unbenommen, eine Vergütung des Auftragnehmers allgemein für Unterstützungshandlungen zugunsten des Auftraggebers zu regeln. Dies kann bspw. für solche Unterstüt-

zungen relevant sein, die nicht dem Leistungsportfolio des Auftragnehmers entsprechen bzw. von Standard-Funktionalitäten einer bereitgestellten Software nicht abgedeckt sind.

9. Interne Kontrollen des Auftragnehmers. Spiegelbildlich zu Art. 28 Abs. 1 DS-GVO hat der Auftragsverarbeiter ausweislich des Vertragsmusters seine technisch-organisatorischen Maßnahmen regelmäßig zu kontrollieren. Besagte Kontrollpflichten werden explizit auch auf die auftragsrelevanten internen Prozesse ausgeweitet (z.B. der Prozess zur Information des Auftraggebers über eine Anfrage von Betroffenen gem. Art. 15 DS-GVO). Immerhin bedarf es auf Seiten des Auftragsverarbeiters einer Vielzahl von Prozessen, um den gesetzlichen sowie vertraglich geforderten Unterstützungshandlungen nachkommen zu können.

10. Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen. Die dem Auftraggeber gesetzlich zustehenden Kontrollhandlungen bedürfen einer Mitwirkung des Auftragsverarbeiters dergestalt, dass dieser die Kontrollhandlungen ermöglicht und unterstützt. Zur Unterstützung des Auftraggebers ist es notwendig, dass dieser durchgängig auf nachvollziehbare und dokumentierte Informationen zurückgreifen kann, um das Schutzniveau der technisch-organisatorischen Maßnahmen beim Auftragnehmer beurteilen zu können. Bei beispielsweise lediglich mündlichen Zusicherungen des Auftragsverarbeiters ist dies regelmäßig nicht möglich.

11. Meldung einer Verletzung des Schutzes personenbezogener Daten. Gibt es beim Auftragnehmer Anhaltspunkte für eine Verletzung des Schutzes personenbezogener Daten, ist er gem. Art. 33 Abs. 2 DS-GVO verpflichtet, den Auftraggeber hierüber unverzüglich in Kenntnis zu setzen. Hierdurch wird der Auftraggeber in die Lage versetzt entscheiden zu können, ob ein meldepflichtiger Sachverhalt gem. Artt. 33/34 DS-GVO gegeben ist.

12. Unterauftragsverhältnisse. Die DS-GVO definiert die Unterauftragsverhältnisse nicht, sondern verweist in Art. 28 Abs. 2 S. 1 DS-GVO auf „weitere Auftragsverarbeiter“, die durch den Auftragsverarbeiter in Anspruch genommen werden. Das Vertragsmuster konkretisiert die Unterauftragsverhältnisse auf solche, die einen unmittelbaren Bezug zur Hauptleistung des Auftragsverarbeiters haben und damit Teil seiner Leistungskette bilden. Die im Vertragsmuster genannten und vom Auftragnehmer in Anspruch genommenen Leitungen, wie bspw. Telekommunikationsleistungen, Post- oder Transportdienstleistungen oder Bewachungsdienstleistungen bilden regelmäßig keinen Bestandteil der Leistungskette und werden durch den Auftragnehmer individuell beauftragt.

Für den Fall vorgesehener Unterauftragsverhältnisse ermöglich das Vertragsmuster dem Auftraggeber solche zu verbieten oder über die Anlage 2 zu erlauben. Für den Fall der Zustimmung für Unterauftragsverarbeiter müssen die gesetzlichen Voraussetzungen hierfür eingehalten werden, die sich insoweit aus Art. 28 Abs. 2-4 DS-GVO ergeben. Ferner sind dem Auftraggeber auf Verlangen die vertraglichen Abreden mit den Unterauftragsverarbeitern auf Verlangen zur Verfügung zu stellen.

Der Wechsel oder die Hinzunahme von Unterauftragsverarbeitern wird an die zusätzliche Bedingung geknüpft, dass der Auftraggeber mindestens 14 Tage vorab schriftlich oder in Textform zu informieren ist und hierdurch die Möglichkeit des Einspruchs erhält.

Der Auftragnehmer ist im Übrigen verpflichtet, die technisch-organisatorischen Maßnahmen beim Unterauftragnehmer vorab der Auftragserteilung und sodann regelmäßig sowie risikoorientiert zu kontrollieren. Hierdurch ist es möglich, das gegenüber dem Auftraggeber vertraglich zugesicherte technisch-organisatorische Schutzniveau innerhalb der Leistungskette des Auftragnehmers zu gewährleisten.

13. Internationale Datentransfers. Übermittlungen personenbezogener Daten in ein Drittland bedürfen der vorherigen Weisung des Auftraggebers. (Art. 28 Abs. 3 S. 2 lit. a DS-GVO). Im Übrigen sind die Vorgaben des Kapitel V zur Gewährleistung eines angemessenen Datenschutzniveaus beim Empfänger im Drittland einzuhalten.

Zu beachten ist hierbei, dass eine rechtliche Verpflichtung nach dem Recht eines Drittlandes nicht ausreicht, um eine Datenübermittlung in ein Drittland zu legitimieren (vgl. Art. 48 DS-GVO).

Für den Fall, dass eine Übermittlung personenbezogener Daten in ein Drittland vorgesehen ist, bspw. an Unterauftragnehmer, muss das entsprechende Land im Vertragsmuster unter der Anlage 2 benannt werden. Ferner ist die verwendete Garantie zur Gewährleistung eines angemessenen Datenschutzniveaus zu benennen (z.B. ein Angemessenheitsbeschluss der Kommission oder Standarddatenschutzklauseln für den Drittlandstransfer).

Sollte der Auftragnehmer seitens des Auftraggebers die Weisung erhalten, personenbezogene Daten an einen anderen Empfänger als die bezeichneten Unterauftragsverarbeiter im Drittland zu übermitteln, ist dieser insoweit für die Erfüllung der Zulässigkeitsanforderungen des Kapitels V verantwortlich.

14. Kontrollrechte des Auftraggebers. Gem. Art. 28 Abs. 3 S. 2 lit. h DS-GVO ist der Auftraggeber berechtigt, selbst oder durch beauftragte Prüfer, Inspektionen beim Auftragnehmer durchzuführen. Das Vertragsmuster konkretisiert dieses Recht und gewährt eine Kontrolle im Geschäftsbetrieb des Auftragnehmers mittels Stichproben nach vorheriger, rechtzeitiger Anmeldung. Es ist den Parteien unbenommen, konkrete Fristen für eine Anmeldung im Vertrag vorzusehen. Dem Auftragnehmer ist es möglich, die Einhaltung der Anforderungen der DS-GVO an die technisch-organisatorischen Maßnahmen mittels eingehaltener Standards, Verhaltensregeln oder über Zertifizierungen nachzuweisen. Dieser Nachweis darf jedoch nicht dazu führen, dass dem Auftraggeber andere Kontrollrechte entzogen werden, so bspw. über eine Kontrolle im Geschäftsbetrieb des Auftragnehmers. Der Auftraggeber entscheidet, ob ihm die vorgelegten Nachweise des Auftragnehmers ausreichen oder ob weitere Informationen eingeholt werden sollen. Den Vertragsparteien ist es im Übrigen unbenommen, die Kostentragung für Kontrollhandlungen des Auftraggebers vertraglich zu regeln (bspw. die Vergütung von externen Prüfern).

15. Weisungsbefugnis des Auftraggebers. Die weisungsgebundene Verarbeitung personenbezogener Daten ist ein wesentliches Merkmal der Auftragsverarbeitung. Insofern sieht Art. 29 DS-GVO vor, dass der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn sie sind nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet. Zum Nachweis einer weisungsgemäßen Verarbeitung sollen Weisungen des Auftraggebers zumindest in Textform dokumentiert werden. Die Festlegung der initialen Weisung des Auftraggebers für den Auftragnehmer erfolgt durch den Vertrag zur Auftragsverarbeitung, der u.a. Spezifikationen zum Auftragsgegenstand, zu Art und Umfang der Verarbeitung sowie zu einem etwaigen Drittlandstransfer enthält.

16. Hinweis bei rechtswidriger Weisung. In Art. 28 Abs. 3 S. 3 DS-GVO ist die Pflicht enthalten, dass der Auftragsverarbeiter den Auftraggeber unverzüglich zu informieren hat, falls nach seiner Auffassung eine Weisung gegen das Datenschutzrecht verstößt. Es empfiehlt sich an dieser Stelle eine vertragliche Klarstellung, wonach der Auftragnehmer zu einer Aussetzung der Verarbeitung befugt sein soll, bis der Auftraggeber die angezeigte Weisung bestätigt oder diese ändert. Die Einschätzung des Auftragnehmers ist subjektiver Natur und hindert den Auftraggeber nicht an einer anderen Auffassung. Es ist ferner ratsam, die Folgen einer nach Mitteilung des Auftragnehmers aufrecht erhaltenen rechtswidrigen

Weisung des Auftraggebers vertraglich zu regeln (z.B. ein vertragliches Sonderkündigungsrecht des Auftragnehmers).

Der gesetzliche Verweis des Art. 28 Abs. 3 S. 3 DS-GVO auf Art. 28 Abs. 3 S. 2 lit. h DS-GVO bezieht sich auf die dortigen allgemeinen Informationspflichten des Auftragnehmers zur Einhaltung des Art. 28 DS-GVO. Diese sollen den Auftraggeber in die Lage versetzen, über die aktuellen Umstände der Verarbeitung im Bilde zu sein. Die Inhalte dieser Information ergeben sich aus den vertraglichen Mindestinhalten des Art. 28 DS-GVO (technisch-organisatorische Maßnahmen, eingesetzte Unterauftragnehmer, Datenempfänger) und können durch weitere Angaben ergänzt werden (so bspw. Aufbewahrungsfristen auf Seiten des Auftragnehmers oder Funktionsbeschreibungen der eingesetzten Systeme). Die Modalitäten der Informationsflüsse sind im Vertrag zu regeln. Das Vertragsmuster benennt hier bspw. Meldefristen für Änderungen der Unterauftragnehmer sowie Veränderungen der technisch-organisatorischen Maßnahmen beim Auftragnehmer.

17. Löschung und Rückgabe von personenbezogenen Daten. Nach Beendigung der Vertragsbeziehung zwischen Auftraggeber und Auftragnehmer sieht Art. 28 Abs. 3 S. 2 lit. g DS-GVO es vor, dass alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder gelöscht oder zurückgegeben werden, sofern der Auftragnehmer nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur weiteren Speicherung verpflichtet ist. Dokumentationen, die dem Nachweis einer ordnungsgemäßen Verarbeitung personenbezogener Daten im Auftrag dienen, können auch nach Vertragsende durch den Auftragnehmer verarbeitet werden. Dies stellt insofern eine vertragliche Befugnis unabhängig einer gesetzlichen Vorgabe dar und dient der Entlastung des Auftragnehmers.

Gesellschaft für Datenschutz
und Datensicherheit e.V.

Ansprechpartner: RA Steffen Weiß, LL.M.

Satz: C. Wengenroth, GDD-Geschäftsstelle, Bonn

Herausgeber:
Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.)
Heinrich-Böll-Ring 10
53119 Bonn
Tel.: +49 0228 96 96 75-00
Fax: +49 0228 96 96 75-25
www.gdd.de
info@gdd.de

Stand:
Version 2.0 (Dezember 2020)