Grundgerüst Auftragsdatenverarbeitungsvertrag nach Art. 28 DS-GVO

Vorbemerkungen

Das nachfolgende Grundgerüst eines Auftragsverarbeitungsvertrages gibt die wesentlichen Bestandteile eines Auftragsverarbeitungsvertrages nach Art. 28 DS-GVO wieder. Die Ausführungen sind nicht abschließend, sondern als Gedankenstütze/Formulierungshilfe gedacht. Das Grundgerüst bedarf abhängig vom konkreten Inhalt der jeweiligen Auftragsverarbeitung, insbesondere der zu verarbeitenden Daten, gegebenenfalls Änderungen, Weglassungen und/oder Ergänzungen.

In einigen Passagen werden Alternativvorschläge unterbreitet, die der Anpassung dienen, in anderen Passagen verweist das Grundgerüst auf gesonderte, vom konkreten Einzelfall inhaltlich abhängige Anlagen zur Ergänzung. Das Grundgerüst ist Anwenderneutral ausgestaltet, so dass es insbesondere hinsichtlich der Passagen zur Haftung und den Rechten/Pflichten der Parteien, je nach Verwender (Auftraggeber <-> Auftragnehmer) gegebenenfalls Änderungen, Weglassungen und/oder Ergänzungen bedarf.

Das nachfolgende Grundgerüst eines Auftragsdatenverarbeitungsvertrages stellt keine zivilrechtliche Beratung durch den GWW dar. Es soll lediglich als Orientierungshilfe dienen bezüglich der sich aus Art.28 DS-GVO ergebenden Informationspflichten, ein Anspruch auf Vollständigkeit wird ausdrücklich nicht erhoben. Aufgrund des sich je nach Verarbeitung und Verarbeitungszweck ändernden Umfang der Regelungsbereiche eines Auftragsverarbeitungsvertrages bedarf es vor Verwendung einer Einzelfallprüfung, inwieweit das Grundgerüst im Einzelfall noch zu ändern und ergänzen ist!

Auftragsverarbeitung gemäß Art. 28 DS-GVO

Vereinbarung
zwischen der

_____
Straße Nr. PLZ Stadt
- Verantwortlicher – nachstehend Auftraggeber genannt -

und dem/der

_____ GmbH
Straße Nr., PLZ Stadt
- Auftragsverarbeiter - nachstehend Auftragnehmer genannt-

A.

1. Dieser Vertrag enthält nach dem Willen der Parteien und insbesondere des Auftraggebers den schriftlichen Auftrag zur Auftragsdatenverarbeitung bzw. den Vertrag i.S.d. Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO) und regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Datenverarbeitung.

2. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die in diesem Vertrag und /oder in der Leistungsvereinbarung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DS-GVO).

3. Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

B.

1. Gegenstand des Auftrags

Gegenstand des Auftrags ist die Durchführung der nachfolgend im Einzelnen aufgeführten Aufgaben durch den Auftragnehmer

- ……..
- … (konkrete Definition der Aufgaben und Dienstleistungen)…
- ……..

2. Dauer des Auftrages

[Alt.1:] Dieser Auftrag beginnt am …… und endet am …….. .

oder

[Alt.2:] Der Auftrag wird auf unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist von drei Monaten zum 30.06. oder 31.12 gekündigt werden.

Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt. Ein Recht zur fristlosen Kündigung besteht insbesondere, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder diesen Vertrag vorliegt.

3. Datenverarbeitung im Rahmen des Vertrages

a) Art und Zweck der vorgesehenen Verarbeitung von Daten

……

……

(Beschreibung von Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer; ggfls. Verweis auf Leistungsvereinbarung)

b) Ort der Leistungserbringung /Datenverarbeitung

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.

Sollte eine Verlagerung der Datenverarbeitung in ein Drittland in Betracht kommen, ist folgender Passus zu ergänzen:

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

Das angemessene Schutzniveau in …… (Land)…….. ist festgestellt durch einen Angemessenheitsbeschluss der Kommission [Art. 45 Abs. 3 DS-GV]);

oder

Das angemessene Schutzniveau in ……(Land)…….. wird hergestellt durch

- *verbindliche interne Datenschutzvorschriften [Art. 46 Abs. 2 b) i.V.m. Art. 47 DS-GVO];*
- *Standarddatenschutzklauseln [Art. 46 Abs. 2 c) und d) DS-GVO];*
- *genehmigte Verhaltensregeln [Art. 46 Abs. 2 lit. e i.V.m. Art. 40 DS-GVO];*
- *einen genehmigten Zertifizierungsmechanismus [Art. 46 Abs. 2 lit. f i.V.m. Art.42 DS-GVO].*
- *sonstige Maßnahmen: …….. [Art. 46 Abs 2 lit. a, Abs. 3 lit. a und lit.b DS-GVO]*

c) Art der Daten

Die im Rahmen dieses Vertrages verarbeiteten personenbezogenen Daten unterfallen folgenden Datenarten/-kategorien

……

…..……

(Aufzählung und evtl. Beschreibung der Datenkategorien: Personendaten, Adressdaten, Kommunikationsdaten, Vertragsstammdaten, Vertragsabrechnungsdaten,….)
(entsprechend der Definition von Art.4 Nr.1, Nr.13, Nr.14 und Nr.15 DS-GVO)

d) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

……..……
…..……
(Aufzählung und evtl. Beschreibung der Personenkategorien: Beschäftigte, Kunden, Lieferanten, Handelsvertreter, Interessenten,….)

4. Schutzmaßnahmen des Auftragnehmers

a) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

b) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind. Der Auftragnehmer stellt dem Auftraggeber auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung.

c) Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern. Die vom Auftraggeber übergebenen Daten sind von sonstigen Datenbeständen strikt zu trennen.

d) In seinem Verantwortungsbereich stellt der der Auftragnehmer durch innerbetriebliche Organisation und Maßnahmen sicher, dass diese den besonderen Anforderungen des Datenschutzes entsprechen. Er trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DS-GVO (TOM-Maßnahmen), insbesondere mindestens die in Anlage __ aufgeführten Maßnahmen der Kontrolle von Zutritt, Zugang, Zugriff, Weitergabe, Eingabe und Verfügbarkeit und Trennung.

e) Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

f) Dem Auftragnehmer als auch den von ihm beschäftigten Personen ist es untersagt, bei der Datenverarbeitung personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden entsprechend umfassend (Nachvertraglich) zur Vertraulichkeit verpflichtet. Der Auftragnehmer hat durch entsprechende Maßnahmen die Einhaltung dieser Vertraulichkeitsverpflichtung sicherstellen und dem Auftraggeber auf Verlangen den Abschluss der Vereinbarung und die weiteren Maßnahmen in geeigneter Weise nachzuweisen.

g) 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.

h) Sollte der Auftragnehmer datenschutzrechtliche Bedenken bezüglich einer Weisung des Auftraggebers haben, informiert er diesen unverzüglich hierüber und weist auf die Bedenken hin. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

i) Der Auftragnehmer ist verpflichtet, den Auftraggeber unverzüglich bei Störungen, bei Verdacht auf Datenschutzverletzungen und/oder sicherheitsrelevanten Vorfälle, der Verletzung vertraglicher Verpflichtungen, oder anderen Unregelmäßigkeiten, die die Verarbeitung der personenbezogenen Daten für den Auftraggeber betreffen, schriftlich oder in Textform zu unterrichten. Die Verpflichtung gilt für Verstöße des Auftragnehmers, der bei ihm beschäftigten Personen oder Dritten gleichermaßen. Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen. Er informiert den Auftraggeber hierüber umfassend und ersucht um weitere Weisungen. Meldungen nach Art.33 oder Art.34 DS-GVO wird der Auftraggeber nur nach ausdrücklicher Weisung durch den Auftraggeber abgeben.

j) Der Auftragnehmer und gegebenenfalls sein Vertreter sind verpflichtet ein Verfahrensverzeichnis gem. Art. 30 DS-GVO zu führen, in dem alle Kategorien der im Auftrag des Auftraggebers durchgeführten Verarbeitungstätigkeiten aufgeführt sind. Der Auftragnehmer wirkt darüber hinaus an der Erstellung des Verfahrensverzeichnisses des Auftraggebers mit, indem er diesem zumindest die jeweils erforderlichen Angaben zu den einzelnen Verarbeitungstätigkeiten mitteilt.

5. Rechte und Pflichten des Auftraggebers (Weisungsrecht)

a) Der Auftraggeber ist alleinig für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO verantwortlich. Der Auftragnehmer ist jedoch verpflichtet, evtl. Anfragen, sofern sie an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

b) Der Auftraggeber ist berechtigt, vor Beginn der Verarbeitung und sodann in regelmäßigen Abständen die Einhaltung des vertraglich vereinbarten Schutzniveaus, insbesondere der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überprüfen. Die Überprüfung kann durch Vorlage von vorhandenen Testaten, Zertifizierungen oder internen Prüfungen oder durch Einholung von Auskünften des Auftragnehmers erfolgen. Darüber hinaus hat der Auftraggeber das Recht, die technischen und organisatorischen Maßnahmen des Auftragnehmers nach terminlicher Abstimmung selbst zu prüfen bzw. durch einen sachkundigen Dritten prüfen zu lassen. Die Kontrollen sind mit Rücksicht auf die Betriebsabläufe des Auftragnehmers durchzuführen.

c) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem nachweisbaren elektronischen Format festzulegen.

d) Die Parteien dieses Vertrages legen in Anlage ___ die weisungsberechtigten Personen des Auftraggebers sowie die Weisungsempfänger beim Auftragnehmer, sowie die zu nutzenden Kommunikationswege fest.

e) Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem nachweisbaren elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

f) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt. Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen

6. Technisch-organisatorische Maßnahmen (TOM)

a) Die Parteien haben im Vorfeld der Auftragsvergabe die erforderlichen technischen und organisatorischen Maßnahmen zur Verarbeitung der personenbezogenen Daten festgelegt, insbesondere auch die Anforderungen an die Dokumentation der TOM und deren Einhaltung. Die vereinbarten Maßnahmen sind im Datenschutzkonzept - Anlage __ - festgeschrieben und Bestandteil dieses Vertrages.

b) Es obliegt dem Auftragnehmer die Sicherheit gem. Art. 28 Abs. 3 c), Art. 32 DS-GVO unter Berücksichtigung des konkreten Risikos für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen herzustellen und ein für die konkrete Auftragsverarbeitung angemessenes Schutzniveau zu gewährleisten. Die zu treffenden Maßnahmen sind unter den Vorgaben des Art. 32 Abs.1 DS-GVO insbesondere bezüglich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme zu treffen.

c) *Die Bewertung des Risikos samt der Auswahl der geeigneten technischen und organisatorischen Maßnahmen des Auftragnehmers wurden am ..... durch folgende unabhängige externe Stellen auditiert/zertifiziert gemäß den Regelungen nach Art. 42:*

.....

Diese vollständigen Prüfunterlagen und Auditberichte können vom Auftraggeber jederzeit eingesehen werden.

oder:

Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DS-GVO). Das Ergebnis samt vollständigem Auditbericht ist dem Auftraggeber mitzuteilen.

7. Einsatz von Subunternehmern

[Alt. 1:] Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen nicht zur Begründung von Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt.

[Alt 2:] Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in Anlage __ genannten Subunternehmer durchgeführt.

a) *Die Beauftragung von Subunternehmern ist dem Auftragnehmer nur nach ausdrücklicher schriftlicher Genehmigung des Auftraggebers gestattet. Diesem ist vor Genehmigung Name, Anschrift und vorgesehene Tätigkeit des möglichen Subunternehmers mitzuteilen.*

b) *Der Auftragnehmer ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit insbesondere im Hinblick auf die von diesen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO auszuwählen. Der Auftragnehmer hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) direkt gegenüber den Subunternehmern wahrnehmen kann.*

c) *Eine Beauftragung von Subunternehmern in einem Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.*

d) *Der Auftragnehmer ist erst befugt Daten an den Subunternehmer weiterzuleiten, wenn dieser die Verpflichtungen nach Art. 29 und Art. 32 abs.4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat.*

e) *Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.*

8. Anfragen und Rechte Betroffener

a) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 sowie 32 und 36 DS-GVO.

b) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist den Betroffenen unverzüglich an den Auftraggeber und wartet dessen Weisungen ab.

9. Haftung

a) Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

b) Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist.

10.Vergütung

Die Vergütung des Auftragnehmers wird gesondert vereinbart.

11.Beendigung des Auftrages

a) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Auftrages oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung bzw. Vernichtung (DIN 32757, 66399) noch vorhandener Daten zu führen.

b) Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren.

c) Von der Verpflichtung zur Löschung sind die Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) ausgenommen, diese sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

d) Der Auftragnehmer ist verpflichtet, auch über das Ende des Auftrages hinaus die ihm im Zusammenhang mit dem Auftrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Auftrages hinaus solange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

12. Schlussbestimmungen

a) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

b) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

c) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

d) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist […].

_____, den _____ _____, den _____

_____ _____

- Auftraggeber - - Auftragnehmer -