

Eva Maria Hajicek - Stefan Steinkogler - Sascha Jung -
Albert Scherzer | Muster | Vertragsmuster

Dokument-ID: 984482

Datenschutzvereinbarung – Auftragsverarbeitung/Subauftragsverarbeitung

... [Datum]

Datenschutzvereinbarung

Gem Art 28 DSGVO

zwischen

... [Name der natürlichen Person/Namensbezeichnung nach Firmenbuch-Verantwortlicher]

... [Anschrift]

nachstehend „Verantwortlicher“ genannt

und

... [Name der natürlichen Person/Namensbezeichnung nach Firmenbuch-Auftragsverarbeiter]

... [Anschrift]

nachstehend „Auftragsverarbeiter“ genannt

Der Verantwortliche und der Auftragsverarbeiter haben folgenden Vertrag abgeschlossen: ... [Vertragsbezeichnung],
... [Datum] (nachstehend „Dienstleistungsvertrag“ genannt).

Gem Art 28 Abs 3 DSGVO ist der Verantwortliche verpflichtet, mit dem Auftragsverarbeiter eine Vereinbarung über die Verarbeitung von personenbezogenen Daten zu schließen. Mit dieser Vereinbarung kommt der Verantwortliche dieser Verpflichtung nach.

Der Auftragsverarbeiter verpflichtet sich, sämtliche Vorgaben der DSGVO in seiner jeweils geltenden Fassung und der sonstigen datenschutzrechtlich spezifischen Materiengesetze und Verordnungen zu beachten.

Variante 1:

In diesem Zusammenhang werden die folgenden datenschutzrechtlichen Verpflichtungen festgehalten (Art 28 Abs 3 DSGVO):

Variante 2: Wenn der Dienstleistungsvertrag gleichzeitig mit der Datenschutzvereinbarung geschlossen wird

Im Zusammenhang mit dem ... [Vertrag] (nachstehend „...“ [Bezeichnung] genannt) werden die folgenden datenschutzrechtlichen Verpflichtungen festgehalten (Art 28 Abs 3 DSGVO):

Variante 3: Subauftragsverarbeitung

zwischen

... [Name der natürlichen Person/Namensbezeichnung nach Firmenbuch- Verantwortlicher]

... [Anschrift]

nachstehend „Auftragsverarbeiter“ genannt

und

... [Name der natürlichen Person/Namensbezeichnung nach Firmenbuch-Auftragsverarbeiter]

... [Anschrift]

nachstehend „Subauftragsverarbeiter“ genannt

Der Verantwortliche und der Auftragsverarbeiter haben folgenden Vertrag abgeschlossen: ...

[Vertragsbezeichnung], ... [Datum] (nachstehend „Dienstleistungsvertrag“ genannt). Der Verantwortliche hat am ... [Datum] das Hinzuziehen eines weiteren Auftragsverarbeiters genehmigt. Der Auftragsverarbeiter und der Subauftragsverarbeiter haben folgenden Vertrag abgeschlossen: ... [Vertragsbezeichnung], ... [Datum] (nachstehend „Subdienstleistungsvertrag“ genannt).

Gem Art 28 Abs 3 DSGVO ist der Verantwortliche verpflichtet, mit dem Auftragsverarbeiter eine Vereinbarung über die Verarbeitung von personenbezogenen Daten zu schließen. Dieser Verpflichtung ist der Verantwortliche mit Abschluss der Datenschutzvereinbarung mit dem Auftragsverarbeiter: ... [Datum] nachgekommen. Gem Art 28 Abs 4 DSGVO ist der Auftragsverarbeiter verpflichtet, mit dem Subauftragsverarbeiter eine Vereinbarung über die Verarbeitung von personenbezogenen Daten zu schließen. Dieser Verpflichtung ist der Auftragsverarbeiter mit Abschluss dieser Datenschutzvereinbarung nachgekommen.

Mit dieser Vereinbarung kommt der Verantwortliche dieser Verpflichtung nach.

Der Subauftragsverarbeiter verpflichtet sich, sämtliche Vorgaben der DSGVO in seiner jeweils geltenden Fassung und der sonstigen datenschutzrechtlich spezifischen Materiengesetze und Verordnungen zu beachten. 1564671375410

1. Auftrag

Wesentlicher Inhalt der vorliegenden Vereinbarung ist die Verarbeitung von personenbezogenen Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen zur Erbringung von Dienstleistungen zum Zweck der ... [genaue und ausführliche Bezeichnung des Zwecks der Verarbeitung der Daten].

2. Datenverarbeitung

a) Durchzuführende Tätigkeit

Im Einzelnen sind vom Auftrag folgende durchzuführende Tätigkeiten umfasst:

... [genaue und ausführliche Darstellung der Verarbeitungstätigkeiten und der Dienstleistungen in Arbeitsschritten/Arbeitspaketen]

b) Datenarten

Zur Durchführung der vereinbarten Tätigkeit werden aus der Datenverarbeitung des Verantwortlichen an den Auftragsverarbeiter folgendermaßen überlassen:

... [Verweis auf in der Anlage befindliche Liste der zu verarbeitenden Daten, alternativ auch Verweis auf einen (Dienstleistungs)Vertrag, in welchem genau beschrieben wird um welche Daten es sich hierbei handelt.

Alternativ kann man die folgende Liste hier oder als Beilage einfügen, wenn man sie als Beilage einfügt, dann muss man hier auf die Beilage verweisen]

Kategorien

Datenkategorien:

betroffener

Personen:

... [zB Mitarbeiter, ... [zB Name, Adresse, Telefonnummer, Kundennummer etc]

Kunden,
Ansprechpersonen
von Kunden,
Lieferanten,
Zielgruppe etc]

... ..

Im Falle von Änderungen der zu verarbeitenden Datenarten und Datenkategorien werden diese vom Verantwortlichen unverzüglich dem Auftragsverarbeiter schriftlich zur Kenntnis gebracht. Sofern der Auftragsverarbeiter binnen 14 Tagen nicht widerspricht, gelten diese Änderungen ab Kenntnissgabe.

c) Datentransfer an den Auftragsverarbeiter

Hinsichtlich des Datentransfers wird Folgendes vereinbart:

... [Hier folgt die Vereinbarung wie die Daten übermittelt werden, hier sind insbesondere die gesetzlichen Modi zu beachten zB für Gesundheitsdaten im Gesundheitstelematikgesetz, falls kein Modus festgelegt ist zB: Mittels PGP codiert, vom Verantwortlichen auf Datenträgern oder via Internet übergeben etc]

d) Pflichten des Auftragsverarbeiters

Es wird vereinbart, dass folgende Verpflichtungen des Auftragsverarbeiters sich auf alle Daten beziehen, auch hinsichtlich jener, welche nicht personenbezogen sind und über die der Auftragsverarbeiter nicht oder nicht alleine verfügen darf.

Der Auftragsverarbeiter übernimmt folgende Verpflichtungen:

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen. Dies gilt auch für die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation. Eine Verarbeitung ohne dokumentierte Weisung ist nur zulässig, wenn der Auftragsverarbeiter hierzu durch das Recht der Europäischen Union oder das Recht eines Mitgliedstaates verpflichtet ist. In diesem Fall informiert der Auftragsverarbeiter den Verantwortlichen vor Beginn der Verarbeitung über die rechtliche Verpflichtung, sofern das betreffende Recht eine solche Information nicht aus wichtigen Gründen des öffentlichen Interesses untersagt.
2. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Europäischen Union oder eines Mitgliedstaates verstößt. Der Auftragsverarbeiter ist berechtigt, die Durchführung der betreffenden Weisung auszusetzen, bis der Verantwortliche sie bestätigt, ändert oder zurücknimmt. Eine Verarbeitung für eigene Zwecke des Auftragsverarbeiters ist unzulässig. Bestimmt der Auftragsverarbeiter entgegen dieser Vereinbarung selbst die Zwecke und Mittel einer Verarbeitung, gilt er hinsichtlich dieser Verarbeitung gemäß Art 28 Abs 10 DSGVO als Verantwortlicher.
3. Der Auftragsverarbeiter trifft alle gem Art 32 DSGVO erforderlichen technischen und organisatorischen Sicherheitsmaßnahmen um einen rechtskonformen Schutz der personenbezogenen Daten der Betroffenen zu bieten. Sämtliche hierfür gesetzten Maßnahmen werden dem Verantwortlichen in geeigneter Weise zur Kenntnis gebracht. Es gelten die in Anlage ./A beschriebenen technischen und organisatorischen (Sicherheits-)maßnahmen, aus ihnen ergibt sich das vom Auftragsverarbeiter geschuldete Mindestschutzniveau. Die technischen und/oder organisatorischen (Sicherheits-)maßnahmen können im Laufe des Vereinbarungsverhältnisses der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, sofern dies keine Unterschreitung des festgelegten Schutzniveaus bewirkt.
4. Der Auftragsverarbeiter wird die im Auftrag des Verantwortlichen verarbeiteten Daten strikt von sonstigen Daten bzw Datenbeständen trennen.
5. Für die vereinbarungsgegenständlichen Tätigkeiten werden ausschließliche Mitarbeiter herangezogen, welche zur Einhaltung der Geheimhaltung von personenbezogenen Daten bzw der Vertraulichkeit vor Verarbeitung bzw Kenntnis dieser Daten verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art 28 Abs 3 lit b DSGVO).
6. Eine Verarbeitung der vereinbarungsgegenständlichen Daten durch weitere Auftragsverarbeiter (nachstehend „Subauftragnehmer“ genannt), insbesondere außerhalb des räumlichen Anwendungsbereichs der DSGVO

- (sogenannten Drittländern), ist nur mit ausdrücklicher vorheriger schriftlicher Zustimmung des Verantwortlichen rechtmäßig. Der Auftragsverarbeiter schließt mit jedem genehmigten Subauftragsverarbeiter vor Beginn der Verarbeitung einen schriftlichen Vertrag oder ein anderes verbindliches Rechtsinstrument. Darin sind dem Subauftragsverarbeiter dieselben datenschutzrechtlichen Pflichten aufzuerlegen, die nach dieser Vereinbarung für den Auftragsverarbeiter gelten. Dies betrifft insbesondere die Weisungsbindung, die Vertraulichkeit, die technischen und organisatorischen Maßnahmen, die Unterstützungspflichten, die Löschung oder Rückgabe der Daten, die Kontrollrechte und die Anforderungen an Drittlandübermittlungen.
7. Der Auftragsverarbeiter darf nur Subauftragsverarbeiter einsetzen, die hinreichende Garantien für eine DSGVO-konforme Verarbeitung bieten. Er bleibt gegenüber dem Verantwortlichen für die Erfüllung der Pflichten des Subauftragsverarbeiters voll verantwortlich.
 8. Die Beauftragung eines weiteren Subauftragsverarbeiters durch einen genehmigten Subauftragsverarbeiter ist nur mit vorheriger schriftlicher Genehmigung des Verantwortlichen und unter Auferlegung derselben datenschutzrechtlichen Pflichten zulässig.
 9. Der Auftragsverarbeiter hat die Einhaltung der Subauftragnehmer nach dieser Vereinbarung treffenden (Datenschutz-)Pflichten regelmäßig zu prüfen, die Prüfergebnisse nachvollziehbar und vollständig zu dokumentieren und über Anfrage des Verantwortlichen diesem die Dokumentation uneingeschränkt vorzulegen.
 10. Kommt der Subauftragnehmer seinen (Datenschutz-)Pflichten nicht nach, so haftet hierfür der Auftragsverarbeiter gegenüber dem Verantwortlichen.
 11. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Beantwortung der datenschutzrechtlichen Anfragen im Sinne des Kapitel III der DSGVO von betroffenen Personen, sodass es dem Verantwortlichen möglich ist die gesetzliche Frist einzuhalten (Art 28 Abs 3 lit e DSGVO).
 12. Der Verantwortliche ist berechtigt, die Einhaltung sämtlicher maßgeblichen datenschutzrechtlichen Vorschriften sowie die Einhaltung der Bestimmungen dieser Vereinbarung selbst oder durch Dritte beim Auftragsverarbeiter zu kontrollieren. Dieses Kontrollrecht umfasst insbesondere das Recht zur Einholung entsprechender Auskünfte, zu deren Erteilung der Auftragsverarbeiter verpflichtet ist, sowie das Recht, sich entsprechende Belege/Zertifikate oder sonstige Bescheinigungen Dritter vorlegen zu lassen die entsprechend als Nachweis dienen. Über Aufforderung hat der Auftragsverarbeiter sämtliche Informationen zur Verfügung zu stellen, die erforderlich sind, um die Einhaltung der Pflichten nach Art 28 DSGVO nachzuweisen. Er ermöglicht Kontrollen und Überprüfungen einschließlich Inspektionen durch den Verantwortlichen oder einen von diesem beauftragten Prüfer und wirkt an diesen mit. Der Auftragsverarbeiter stellt durch seine Verträge mit den Subauftragsverarbeitern sicher, dass die für eine Überprüfung erforderlichen Informationen zur Verfügung gestellt werden und erforderlichenfalls angemessene Kontrollen bei den Subauftragsverarbeitern ermöglicht werden. Berufsrechtliche Verschwiegenheitspflichten, Geschäftsgeheimnisse und Sicherheitsinteressen sind durch geeignete organisatorische Maßnahmen zu schützen, dürfen das gesetzliche Kontrollrecht jedoch nicht praktisch ausschließen.
 13. Kontrollen beim Auftragsverarbeiter bzw beim Subauftragnehmer haben nach angemessener Vorankündigung zu normalen Geschäftszeiten und unter möglichst geringer Störung des Geschäftsbetriebs des Auftragsverarbeiters bzw Subauftragnehmers zu erfolgen. Der vorstehende Satz gilt nicht für dringliche Fälle, welche der Verantwortliche nachzuweisen hat.
 14. Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten des Verantwortlichen (ungeachtet, ob dieser data breach auf den Auftragsverarbeiter oder den Verantwortlichen oder einen sonstigen Dritten zurückzuführen ist) bekannt wird, wird er diese dem Verantwortlichen unverzüglich melden, die bekanntgewordene Verletzung einschließlich ihrer Auswirkungen und der getroffenen Abhilfemaßnahmen dokumentieren und dem Verantwortlichen diese Dokumentation zur Verfügung stellen. Darüber hinaus wird er den Verantwortlichen bei dessen Meldung allfälliger data breaches an die zuständige Aufsichtsbehörde unterstützen und alle damit im Zusammenhang stehenden Informationen erteilen. Weiter wird er dem Verantwortlichen alle notwendigen Informationen bereitstellen, die allenfalls notwendig sind, damit dieser die vom data breach betroffene(n) Person(en) unverzüglich von der Verletzung benachrichtigen kann.
 15. Im Zusammenhang mit der beauftragten Datenverarbeitung wird der Auftragsverarbeiter den Verantwortlichen – soweit gesetzlich erforderlich – bei der Erstellung und Aktualisierung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei der Durchführung der Datenschutzfolgeabschätzung unterstützen und alle dafür notwendigen Angaben machen und Informationen erteilen.

3. Ort der Datenverarbeitung

[Wenn außerhalb der EU/EWR eine Datenverarbeitung stattfindet, müssen die erhöhten Schutzvorschriften iSd Art 44 ff DSGVO eingehalten werden. Daher sollte der Ort der Verarbeitung explizit festgehalten werden. Im Falle einer Verarbeitung im Drittland sollte eine Rechtfertigung vorliegen. Daher ergeben sich folgende Varianten:]

- Vereinbarungsgegenständliche Daten werden ausschließlich innerhalb der EU/EWR verarbeitet.
- Die Verarbeitung vereinbarungsgegenständlicher Daten werden in ... [Nennung des Staates bzw der Staaten] vorgenommen. Das Datenschutzniveau gilt in diesem Staat/in diesen Staaten aus folgenden Gründen als angemessen:
... [Nennung des Angemessenheitsbeschlusses gem Art 45 DSGVO, Vorlage der geeigneten Garantien, genehmigter Verhaltensregeln, verbindlicher interner Datenschutzklauseln, Ausnahme gem Art 49 DSGVO etc]

4. Vereinbarungsdauer und Verpflichtungen nach Beendigung dieser Vereinbarung

[Verantwortlicher und Auftragsverarbeiter können die Dauer dieser Vereinbarung folgendermaßen festlegen: einmalige Verarbeitung, befristet, unbefristet oder an den Hauptvertrag gebunden:]

- Diese Vereinbarung endet automatisch nach einmaliger Durchführung der Verarbeitung (siehe auch ... Nennung des Dienstleistungsvertrages ...) [oder]
- Die vereinbarungsgegenständliche Befristung ist vom ... [Beginn der Frist] bis ... [Ende der Frist bzw Verweis auf die Beendigung des Dienstleistungsvertrages] [oder]
- Diese Vereinbarung wurde auf unbestimmte Zeit geschlossen und kann nach einer Frist von ... [Kündigungsfrist] zum ... [Kündigungstermin] gekündigt werden [oder]
- Diese Vereinbarung ist in ihrer Dauer von dem ihm zugrundeliegenden Dienstleistungsvertrag abhängig.

Ungeachtet des Fortbestands des Dienstleistungsvertrags ist der Verantwortliche berechtigt, diese Vereinbarung ohne Einhaltung von Kündigungsfristen oder Kündigungsterminen aus wichtigem Grund mit sofortiger Wirkung zu beenden.

Bei Beendigung der Vereinbarung (oder auch jederzeit vorher über entsprechendes Verlangen des Verantwortlichen) wird der Auftragsverarbeiter die im Auftrag verarbeiteten Daten (einschließlich allfälliger Kopien) nach freier Wahl des Verantwortlichen entweder selbst vernichten oder zur Gänze an den Verantwortlichen übergeben, sofern dem keine gesetzliche Pflicht zur Aufbewahrung entgegensteht. Die Vernichtung hat in einer Weise zu erfolgen, dass eine auch bloß teilweise Wiederherstellung der gelöschten Daten nicht oder nur mit technisch und wirtschaftlich unverhältnismäßigem Aufwand möglich ist.

Der Auftragsverarbeiter ist gleichermaßen verpflichtet, die Vernichtung oder Übergabe durch allfällige Subauftragnehmer herbeizuführen.

Im Fall der Datenvernichtung hat der Auftragsverarbeiter dem Verantwortlichen die ordnungsgemäße Durchführung der Datenvernichtung schriftlich zu bestätigen und nachzuweisen.

5. Geheimhaltung

Der Verantwortliche und der Auftragsverarbeiter verpflichten sich zur strikten Geheimhaltung aller Geschäftsgeheimnisse sowie sonstiger Unterlagen und Informationen, die ihnen aufgrund ihrer Tätigkeit entsprechend dieser Vereinbarung bekannt werden, dies auch nach Beendigung dieser Vereinbarung.

6. Vergütung

Für die Erbringung der Leistungen unter dieser Vereinbarung erfolgt keine gesonderte Vergütung oder Kostenerstattung zugunsten des Auftragsverarbeiters. Die Vereinbarungsparteien sind sich einig, dass die Leistungen unter dieser Vereinbarung durch das im Dienstleistungsvertrag vereinbarte Entgelt mitabgegolten sind.

7. Allgemeine Bestimmungen

Diese Datenschutzvereinbarung ersetzt allfällige frühere Datenschutzverträge.

Änderungen und Ergänzungen dieser Vereinbarung einschließlich dieses Punktes bedürfen der Schriftform sowie der Unterschrift beider Vereinbarungsparteien.

Auf alle Rechtsfragen aus oder im Zusammenhang mit dieser Vereinbarung einschließlich der Frage seines gültigen Zustandekommens und seiner Vor- und Nachwirkungen ist ... [Rechtswahl] Recht unter Ausschluss seiner Verweisungsnormen anzuwenden.

Der Auftragsverarbeiter ist verpflichtet iSv Art 82 Abs 5 DSGVO den Verantwortlichen betreffend aller Ansprüche, welche in einem Zusammenhang mit dieser Vereinbarung stehen, schad- und klaglos zu halten.

Der Verantwortliche und der Auftragsverarbeiter vereinbaren für sämtliche Streitigkeiten aus oder im Zusammenhang mit dieser Vereinbarung einschließlich der Frage seines gültigen Zustandekommens und seiner Vor- und Nachwirkungen die ausschließliche Zuständigkeit des jeweils sachlich zuständigen Gerichts in ... [Stadt].

Sollten Teile dieser Vereinbarung oder Inhalte einer in dieser Vereinbarung integrierten Anlage ungültig sein oder werden, so wird dadurch die Wirksamkeit der Vereinbarung im Übrigen nicht berührt. Verantwortlicher und Auftragsverarbeiter werden die unwirksame Bestimmung durch eine wirksame Bestimmung ersetzen, die dem gewollten Zweck der ungültigen Bestimmung sowie dem ursprünglich vereinbarten Vereinbarungsgleichgewicht möglichst nahekommt. Dasselbe gilt auch für allfällige Vereinbarungslücken.

Diese Vereinbarung verfügt über eine Anlage ./A (Technische und organisatorische Maßnahmen), die einen integrierten Bestandteil dieser Vereinbarung bildet.

..., am ...

Anlage ./A Technische und organisatorische Maßnahmen

Folgende technische und organisatorische Maßnahmen wurden vom Auftragsverarbeiter gesetzt:

Zugangskontrolle: Es wurden die notwendigen Maßnahmen gesetzt, welche Unbefugten den Zutritt zu den technischen Einrichtungen verwehren, in welchen die Verarbeitung stattfindet. (Angaben wie zB versperrter Serverraum, protokollierter Zutritt zum Serverraum, Sicherung von Fenstern, Türen, Schachtabdeckungen, Aufzugs- und Filteranlagen, Laptops/PCs/Thin Clients befinden sich in versperrten Räumen, der Zutritt zu den Räumen wird aufgrund eines Berechtigungskonzeptes genehmigt, Sichtbares Tragen eines Ausweises)

Datenträgerkontrolle: Es wurden Maßnahmen gesetzt, welche unbefugtes Lesen, Kopieren, Verändern oder Entfernen von Datenträgern verhindern.

Benutzerkontrolle: Es wurden Maßnahmen gesetzt, welche den Benutzern nach dem „Need-to-know-Prinzip“ Berechtigungen erteilt und Unbefugte keinen Zugriff auf Daten haben. Zugang zu personenbezogenen Daten dürfen nur jene haben, welche persönlich beauftragt sind diese zu verarbeiten – Auftragsprinzip.

Zugriffskontrolle: Es wird gewährleistet, dass ausschließlich Berechtigte Zugang zu personenbezogenen Daten haben. Personenbezogene Daten werden mit Hilfe von Pseudonymisierung und Verschlüsselung vor unbefugten Zugriffen gesichert.

Übertragungskontrolle: Es wird gewährleistet, dass überprüft und festgestellt werden kann, an wen personenbezogene Daten übermittelt oder zur Verfügung gestellt wurden oder werden können.

Eingabekontrolle: Es wird gewährleistet, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem eingegeben worden sind.

Transportkontrolle: Es werden Maßnahmen getroffen, welche verhindern, dass bei der Übermittlung/Transport personenbezogener Daten die Daten von Unbefugten gelesen, kopiert, verändert oder gelöscht werden können. Daten auf mobilen Datenträgern werden nur von Befugten verwendet und transportiert.

Wiederherstellung: Es wird gewährleistet, dass im Störfall die Systeme und Daten wiederhergestellt werden können.

Datenintegrität: Es wird gewährleistet, dass alle Funktionen des Systems zur Verfügung stehen, alle auftretenden Fehlfunktionen gemeldet werden und sämtliche gespeicherten personenbezogenen Daten durch Fehlfunktionen des Systems nicht beschädigt werden können.

Qualitätskontrolle: Es wird gewährleistet, dass die technischen und organisatorischen Maßnahmen regelmäßiger Überprüfungen unterzogen werden und eine Bewertung und Evaluierung der Wirksamkeit dieser Maßnahmen stattfindet.