[Diese Vorlage wird auf folgenden öffentlich geteilt [https://www.iubenda.com/de/help/56461](https://www.iubenda.com/de/help/56461-auftragsverarbeitungsvereinbarung-dsgvo-vorlage)]

# Muster - Auftragsverarbeitungsvereinbarung

## Auftragsverarbeitungsvereinbarung (AVV)

gem. Art. 28 Datenschutzgrundverordnung (DSGVO)

zwischen

................................................................................................

* + dem Verantwortlichen

[falls zutreffend: Vertreter im Sinne von Art. 27 DSGVO:

................................................................................................]

und

.................................................................................................

* + dem Auftragsverarbeiter

[falls zutreffend: Vertreter im Sinne von Art. 27 DSGVO:

................................................................................................]

## 1. Gegenstand, Vertragsdauer, verarbeitete personenbezogene Daten und Kategorien von Betroffenen

(1) Gegenstand

* + Gegenstand dieser AVV ist die Beauftragung des Auftragsverarbeiters durch den Verantwortlichen und die Erteilung von Weisungen hinsichtlich der Verarbeitung personenbezogener Daten. Die vom Auftragsverarbeiter durchzuführenden Verarbeitung ist streng auf die Tätigkeiten beschränkt, die zur Erfüllung des von den Parteien am [Datum einfügen] unterzeichneten Hauptvertrags erforderlich sind [*Datum einfügen*].

[oder

* + Der Auftragsverarbeiter führt die folgenden Verarbeitungstätigkeiten im Auftrag des Verantwortlichen durch:
	**..............................................................................................................**
	**..............................................................................................................**
	**..............................................................................................................**
	**..............................................................................................................**
	**..............................................................................................................]**

(2) Vertragsdauer

* + Die Vertragsdauer dieser AVV entspricht der des Hauptvertrags.

[alternativ: Vertragsdauer angeben]

(3) Kategorien personenbezogener Daten

* + Die Kategorien der verarbeiteten personenbezogenen Daten sind:
		- Stammdaten (Vorname, Nachname, E-Mail)
		- statistische oder andere Daten über das Browsing (z. B. Daten, die von Analyse-Tools usw. verarbeitet werden)
		- Kundenhistorie
		- Abrechnungs-, Rechnungs- und Zahlungsdaten
		- sonstige:….................................................. [*bitte detailliert angeben, insbesondere wenn genetische, biometrische oder andere sensible Daten verarbeitet werden*]

(4) Kategorien Betroffener

* + Die erfassten und verarbeiteten personenbezogenen Daten beziehen sich auf:
		- Kunden
		- potenzielle Kunden
		- Internetnutzer
		- Angestellte, Mitarbeiter, Personalmitglieder
		- interne Berater
		- Auftragnehmer und Vertreter
		- sonstige:….................................................. [*bitte spezifizieren*]

## 2. Datenübermittlung ins Ausland

(1) Der Auftragsverarbeiter **verpflichtet** sich, ohne vorherige schriftliche Genehmigung des Verantwortlichen keine personenbezogenen Daten ins Ausland (d. h. außerhalb des EWR-Gebiets) zu übermitteln. Jegliche Datenübermittlung ins Ausland und die damit verbundenen Verarbeitungstätigkeiten werden unter strikter Einhaltung der dokumentierten und spezifischen Anweisungen des Verantwortlichen durchgeführt.

*[Option 1 keine Datenübermittlung]*

(2) Beide Parteien sind sich darüber einig und vereinbaren, dass die Datenverarbeitungsaktivitäten im Rahmen dieser Vereinbarung nicht außerhalb des EWR stattfinden.

*[alternativ: bei Datenübermittlung ins Ausland]*

(2) Der Verantwortliche nimmt zur Kenntnis, dass er zum Zeitpunkt der Unterzeichnung der vorliegenden Vereinbarung darüber informiert wurde, dass die folgenden Datenverarbeitungsaktivitäten, die vom Auftragsverarbeiter in seinem Auftrag durchgeführt werden, außerhalb des EWR stattfinden werden.
Diese Verarbeitungen, zu denen der Verantwortliche hiermit seine ausdrückliche Zustimmung erteilt, finden in den nachstehend aufgelisteten Staaten und unter strikter Einhaltung der Rechtsgrundlagen für die Datenübermittlung gemäß den Artikeln 45 und ff. DSGVO statt, soweit diese auf die jeweilige Verarbeitungstätigkeit anwendbar sind.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Land** | **Datenverarbeitungstätigkeit** | **Rechtsgrundlage für die Übermittlung** |
| 1 | *z.B. Schweiz* | *z.B. Hosting-Dienst* | *z.B. Angemessenheitsbeschluss* |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |
| 5 |  |  |  |

*(Die wichtigsten Rechtsgrundlagen für die Übermittlung gemäß der DSGVO sind:*

* + *ein Angemessenheitsbeschluss der Europäischen Kommission (Artikel 45 Absatz 3 DSGVO);*
	+ *verbindliche interne Datenschutzvorschriften (Artikel 46 Absatz 2 Buchstabe b in Verbindung mit Artikel 47 DSGVO);*
	+ *Standarddatenschutzklauseln (Artikel 46 Absatz 2 Buchstaben c und d DSGVO);*
	+ *Verhaltensregeln (Artikel 46 Absatz 2 Buchstabe e in Verbindung mit Artikel 40 DSGVO);*
	+ *Zertifizierungsmechanismen (Artikel 46 Absatz 2 Buchstabe f in Verbindung mit Artikel 42 DSGVO).*

*Wählen Sie für jede in der Tabelle aufgeführte Verarbeitungstätigkeit die entsprechende Option aus der obigen Liste aus)*

## 3. Technische und organisatorische Maßnahmen

(1) Der Auftragsverarbeiter verpflichtet sich, vor der Unterzeichnung dieser AVV alle erforderlichen technischen und organisatorischen Sicherheitsmaßnahmen zu ergreifen und dem Verantwortlichen ein Dokument zu übermitteln, in dem alle diese Maßnahmen im Einzelnen beschrieben sind, auch unter besonderer Bezugnahme auf die vorliegende Vereinbarung.

Diese Maßnahmen unterliegen der Prüfung durch den Verantwortlichen und müssen von diesem vorab genehmigt werden. Nach der Genehmigung durch den Verantwortlichen werden diese Sicherheitsmaßnahmen, die wie oben dokumentiert werden, wesentlicher und verbindlicher Bestandteil dieser Vereinbarung kraft Einbeziehung. Sofern sich bei einer Prüfung/einem Audit durch den Verantwortlichen die Notwendigkeit von Änderungen ergibt, werden diese Änderungen im gegenseitigen Einvernehmen vorgenommen.

(2) Der Auftragsverarbeiter garantiert, dass er alle Sicherheitsmaßnahmen gemäß Artikel 28 Absatz 3 Buchstabe c und Artikel 32 DSGVO, insbesondere in Verbindung mit Artikel 5 Absatz 1 und Absatz 2 DSGVO, ergriffen hat. Diese Maßnahmen müssen die Datensicherheit und ein dem Risiko angemessenes Schutzniveau in Bezug auf Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme gewährleisten. Gemäß Artikel 32, Absatz. 1 DSGVO ist bei der Beurteilung der Angemessenheit der getroffenen Sicherheitsmaßnahmen Folgendes zu berücksichtigen: ob die Maßnahmen vernünftigerweise als dem Stand der Technik entsprechend angesehen werden können, die Implementierungskosten, die Art, der Umfang und die Zwecke der Verarbeitung sowie die Wahrscheinlichkeit von Datenverletzungen und die Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen und technologischen Fortschritt und Entwicklung. Der Auftragsverarbeiter kann daher alternative geeignete Maßnahmen ergreifen, die dem Stand der Technik entsprechen. Dabei darf das Sicherheitsniveau der Verarbeitung nicht verringert werden. Wesentliche Änderungen müssen dokumentiert werden.

## 4. Rechte der Betroffenen

(1) Der Auftragsverarbeiter verpflichtet sich zur umfassenden Zusammenarbeit, soweit dies vernünftigerweise möglich ist, um den Verantwortlichen bei der Beantwortung von Anträgen der Betroffenen auf Ausübung ihrer Rechte zu unterstützen.

(2) Insbesondere verpflichtet sich der Auftragsverarbeiter, (**i**) dem Verantwortlichen unverzüglich jeden Antrag der Betroffenen auf Ausübung ihrer Rechte mitzuteilen und, sofern möglich und angemessen, (**ii**) dem Verantwortlichen zu ermöglichen, alle technischen und organisatorischen Maßnahmen zu entwerfen und umzusetzen, die erforderlich sind, um den Anträgen der Betroffenen zu entsprechen.

(3) Unbeschadet der Tatsache, dass der Verantwortliche die Verantwortung für die Beantwortung der Anträge der Betroffenen trägt, kann der Auftragsverarbeiter mit der Erfüllung einiger spezifischer Anträge beauftragt werden, sofern diese Aufgaben keinen unzumutbaren Aufwand des Auftragsverarbeiters erfordern und der Verantwortliche detaillierte schriftliche Anweisungen dazu erteilt.

## 5. Weitere Pflichten des Auftragsverarbeiters

Zusätzlich zur Einhaltung der Bestimmungen dieser AVV verpflichtet sich der Auftragsverarbeiter, alle einschlägigen gesetzlichen Anforderungen zu erfüllen, die in den Artikeln 28 bis 33 DSGVO festgelegt sind.
Zu diesem Zweck garantiert der Auftragsverarbeiter die Einhaltung des Folgenden:

* + **Benennung eines Datenschutzbeauftragten (DSB)**

	Der derzeitige DSB ist:
	(VOLLSTÄNDIGE KONTAKTANGABEN)**.....................................**
	**..............................................................................................................**
	**..............................................................................................................**
	Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über jegliche Änderung des Datenschutzbeauftragten.

	[*oder* Der Auftragsverarbeiter ist nicht verpflichtet, einen Datenschutzbeauftragten zu benennen. Herr/Frau [*Vorname, Nachname, Abteilung, Telefon, E-Mail einfügen*] ist als Kontaktperson im Auftrag des Auftragsverarbeiters benannt.]
	+ [→ nur wenn zutreffend auswählen] **Benennung eines Vertreters in der Union**
	Da der Auftragsverarbeiter außerhalb der EU und des EWR ansässig ist, hat er
	(VOLLSTÄNDIGE KONTAKTANGABEN)**......................................**
	**..............................................................................................................**
	**..............................................................................................................** gemäß Artikel 27 Absatz 1 DSGVO als Vertreter in der Union benannt.
	+ **Vertraulichkeit**
	Die Verarbeitungstätigkeiten im Rahmen dieser AVV dürfen nur von Personen (z. B. Angestellten, Beauftragten oder Mitarbeitern) durchgeführt werden, die vom Auftragsverarbeiter über die angemessene Art und Weise der Datenverarbeitung belehrt und vertraglich zur Vertraulichkeit gemäß Art. 28 Abs. 3 (b) und Art. 32 DSGVO verpflichtet sind. Der Auftragsverarbeiter und jede unter seiner Aufsicht handelnde Person, die Zugang zu personenbezogenen Daten hat, darf diese Daten nur auf Anweisung des Verantwortlichen - einschließlich der gemäß dieser DSGVO erteilten Befugnisse - verarbeiten, es sei denn, sie sind hierzu durch gesetzliche Vorschriften verpflichtet.
	+ **Technische und organisatorische Maßnahmen**
	Implementierung und Einhaltung aller angemessenen technischen und organisatorischen Maßnahmen im Rahmen dieser AVV, insbesondere wie in Art. 32 DSGVO festgelegt. Der Auftragsverarbeiter überwacht regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um sicherzustellen, dass die ihn betreffenden Verarbeitungstätigkeiten im Einklang mit den Anforderungen des geltenden Datenschutzrechts und dem Schutz der Rechte der Betroffenen durchgeführt werden. Der Auftragsverarbeiter gewährt dem Verantwortlichen die Nachprüfbarkeit der technischen und organisatorischen Maßnahmen im Rahmen seiner Kontrollbefugnisse gemäß Absatz 7 dieser Vereinbarung.
	+ **Zusammenarbeit mit den Aufsichtsbehörden**
	Der Verantwortliche und der Auftragsverarbeiter arbeiten auf Anfrage mit der Aufsichtsbehörde zusammen. Der Verantwortliche ist unverzüglich über alle von der Aufsichtsbehörde durchgeführten Kontrollen und Maßnahmen zu informieren, soweit sie sich auf die Tätigkeiten im Rahmen dieser AVV beziehen. Dies gilt auch für den Fall, dass gegen den Auftragsverarbeiter direkt oder als Verfahrensbeteiligter von einer zuständigen Behörde eine Ermittlung wegen Verstößen gegen eine Vorschrift über die Verarbeitung personenbezogener Daten im Zusammenhang mit der Durchführung dieser AVV eingeleitet wird. Insofern der Verantwortliche einer Kontrolle durch die Aufsichtsbehörde, einem Bußgeldverfahren, einer einstweiligen Verfügung oder einem Strafverfahren, einem Haftungsanspruch eines Betroffenen oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Datenverarbeitung durch den Auftragsverarbeiter gemäß dieser AVV ausgesetzt ist, wird der Auftragsverarbeiter alle Anstrengungen unternehmen, um den Verantwortlichen zu unterstützen.

## 6. Unterauftragsverarbeiter

(1) Der Verantwortliche ermächtigt den Auftragsverarbeiter, einen Teil der Verarbeitungstätigkeiten gemäß dieser AVV an Unterauftragsverarbeiter zu delegieren. Die Unterauftragsverarbeiter unterliegen, soweit gesetzlich vorgeschrieben, denselben vertraglichen Verpflichtungen, die sich aus dieser Vereinbarung ergeben, gemäß Art. 28 Abs. 4 DSGVO.

[*Absatz (2) ist fakultativ, nur wenn Unterauftragsverarbeiter bereits beauftragt sind]*

(2) Zum Zeitpunkt der Unterzeichnung dieser Vereinbarung sind sich die Parteien darüber einig und vereinbaren, dass der Auftragsverarbeiter derzeit die folgenden Unterauftragsverarbeiter unter der Voraussetzung einer vertraglichen Vereinbarung gemäß Artikel 28 Absatz 4 DSGVO beauftragt:

|  |  |  |  |
| --- | --- | --- | --- |
|  | Unterauftragsverarbeiter | Anschrift/Land | Delegierte Verarbeitungstätigkeit |
| 1 |  |  |  |
| 2 |  |  |  |

(3) Zwischen den Parteien besteht Einvernehmen darüber, dass die Übermittlung personenbezogener Daten an einen Unterauftragsverarbeiter erst dann erfolgen darf, wenn alle in Absatz 1 genannten Bedingungen für die Benennung von Unterauftragsverarbeitern erfüllt sind.
(4) Der Auftragsverarbeiter muss ein Verzeichnis der Unterauftragsverarbeiter führen und auf dem neuesten Stand halten. Jede Änderung dieser Liste ist dem Verantwortlichen unverzüglich mitzuteilen, wobei der Verantwortliche die Möglichkeit haben muss, Einspruch zu erheben. Im Falle eines Widerspruchs behält sich der Auftragsverarbeiter das Recht vor, den mit dem Verantwortlichen bestehenden Vertrag fristlos zu kündigen.
(5) Der Auftragsverarbeiter trägt die volle Verantwortung und Haftung für die Tätigkeiten seiner Unterauftragsverarbeiter gegenüber dem Verantwortlichen.
(6) Erbringt ein Unterauftragsverarbeiter seine Leistungen außerhalb der EU/des EWR, so hat der Auftragsverarbeiter die Einhaltung der Vorschriften über die Datenübermittlung ins Ausland, wie in Absatz 2 dieser AVV dargelegt, sicherzustellen.

## 7. Audits

(1) Der Verantwortliche hat das Recht, Überprüfungen durchzuführen oder sie von einem von Fall zu Fall benannten Prüfer durchführen zu lassen. Der Prüfer bewertet die Einhaltung dieser AVV in der betrieblichen Tätigkeit des Auftragsverarbeiters anhand von stichprobenartigen Kontrollen, von denen der Auftragsverarbeiter im Voraus in Kenntnis gesetzt wird.
(2) Der Auftragsverarbeiter ermöglicht es dem Verantwortlichen, die Einhaltung seiner Verpflichtungen gemäß Artikel 28 DSGVO zu überprüfen. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf Anfrage die erforderlichen Informationen zu geben und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
(3) Nachweise für die Durchführung solcher Maßnahmen, die nicht nur die Tätigkeiten im Rahmen dieser AVV betreffen, können auch erbracht werden durch:

* + Einhaltung der genehmigten Verhaltensregeln gemäß Artikel 40 DSGVO;
	+ Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Artikel 42 DSGVO;
	+ aktuelle Auditzertifikate, Berichte oder Auszüge aus Berichten unabhängiger Stellen (z.B. Wirtschaftsprüfer, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditor);
	+ eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzauditierung.

(4) Der Auftragsverarbeiter kann dem Verantwortlichen eine angemessene Gebühr für die Durchführung von Überprüfungen in Rechnung stellen.

## 8. Unterstützung des Verantwortlichen

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung der in den Artikeln 32 bis 36 der DSGVO festgelegten Pflichten in Bezug auf die Sicherheit personenbezogener Daten, die Meldung von Datenschutzverletzungen, Datenschutz-Folgenabschätzungen und vorherige Konsultationen, einschließlich:

* Gewährleistung eines angemessenen Sicherheitsstandards durch technische und organisatorische Maßnahmen unter Berücksichtigung der Art, der Umstände und der Zwecke der Verarbeitung, der Wahrscheinlichkeit von Datenverletzungen und der Schwere des sich daraus möglicherweise ergebenden Risikos für natürliche Personen
* Gewährleistung der sofortigen Aufdeckung von Verstößen
* die unverzügliche Meldung von Datenschutzverletzungen an den Verantwortlichen
* Unterstützung des Verantwortlichen bei der Beantwortung von Anträgen der Betroffenen auf Ausübung ihrer Rechte

(2) Der Auftragsverarbeiter kann dem Verantwortlichen eine angemessene Gebühr für Unterstützungsleistungen in Rechnung stellen, die nicht in der Beschreibung der Leistungen enthalten sind und die nicht auf ein Fehlverhalten, Fehler oder Verstöße des Auftragsverarbeiters zurückzuführen sind.

## 9. Weisungsbefugnisse des Verantwortlichen

(1) Der Auftragsverarbeiter darf personenbezogene Daten im Rahmen dieser AVV nur auf dokumentierte Weisung des Verantwortlichen verarbeiten, es sei denn, er ist nach dem Recht der Union oder eines Mitgliedstaats dazu verpflichtet.
(2) Verlangt der Verantwortliche eine Änderung bei der Verarbeitung personenbezogener Daten, die in den in Abschnitt 2 genannten dokumentierten Anweisungen vorgesehen ist, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich zu informieren, wenn er der Ansicht ist, dass diese Änderungen zu Verstößen gegen die Datenschutzbestimmungen führen könnten. Der Auftragsverarbeiter kann jede Tätigkeit unterlassen, die zu einem solchen Verstoß führen könnte.

## 10. Haftung

(1) Jede Partei dieser AVV verpflichtet sich, die jeweils andere Partei von Schäden oder Aufwendungen freizuhalten, die auf einem eigenen schuldhaften Verstoß gegen diese AVV beruhen, einschließlich eines schuldhaften Verstoßes durch ihre gesetzlichen Vertreter, Unterauftragnehmer, Angestellten oder sonstigen Beauftragten. Darüber hinaus verpflichtet sich jede Partei, die andere Partei von allen Ansprüchen Dritter freizuhalten, die aufgrund oder im Zusammenhang mit einer schuldhaften Verletzung durch die jeweils andere Partei geltend gemacht werden.
(2) Art. 82 DSGVO bleibt davon unberührt.

## 11. Löschung und Rückgabe von personenbezogenen Daten

(1) Der Auftragsverarbeiter darf ohne Wissen und Zustimmung des Verantwortlichen keine Kopien oder Duplikate der Daten erstellen, es sei denn, es handelt sich um Sicherungskopien, soweit diese für die Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind und wenn die Aufbewahrung dieser Daten gesetzlich vorgeschrieben ist.
(2) Nach Beendigung der Leistungserbringung hat der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Rahmen dieser DSGVO erhobenen und verarbeiteten personenbezogenen Daten entweder in einer den Datenschutzbestimmungen konformen Weise zu löschen oder an den Verantwortlichen zurückzugeben, es sei denn, eine anwendbare Rechtsvorschrift schreibt eine weitere Speicherung der personenbezogenen Daten vor.
(3) In jedem Fall kann der Auftragsverarbeiter alle Informationen, die für den Nachweis der Ordnungsmäßigkeit der durchgeführten Verarbeitungstätigkeiten erforderlich sind, über die Beendigung des Vertrags hinaus aufbewahren.
(4) Die unter Punkt (3) genannte Dokumentation wird vom Auftragsverarbeiter gemäß den geltenden gesetzlichen oder anderweitig festgelegten Aufbewahrungsfristen aufbewahrt. Der Auftragsverarbeiter kann die Dokumentation bei Beendigung des Vertrags an den Verantwortlichen aushändigen. In diesem Fall ist der Auftragsverarbeiter von jeder Verpflichtung zur Aufbewahrung dieser Unterlagen befreit.