

---

## Vertrag über die Auftragsverarbeitung personenbezogener Daten gem. Art. 28 Abs. 3 DSGVO

zwischen

Name, Anschrift

(Auftraggeber/Verantwortlicher)

- im Folgenden: Auftraggeber -

und

Name, Anschrift

(Auftragnehmer/Auftragsverarbeiter)

- im Folgenden: Auftragnehmer -

### Haftungsausschluss:

Der vorliegende Mustervertrag dient als Formulierungshilfe und ist entsprechend den Anforderungen an die DSGVO möglichst verständlich formuliert. Jedoch sollten Sie das Muster nur nach sorgfältiger Prüfung und Anpassung auf Ihren spezifischen Einzelfall und nach Ihren eigenen Anforderungen anwenden und ggf. ergänzen und erweitern. Lassen Sie sich im Zweifel rechtlich beraten.

## 1. Grundlage des Vertrags

Dieser Vertrag regelt die datenschutzrechtlichen Verpflichtungen von Auftraggeber und -nehmer (Vertragsparteien) im Rahmen einer Auftragsverarbeitung von personenbezogenen Daten.

Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen der Auftragnehmer, dessen Mitarbeiter oder durch ihn beauftragte Dritte (Unterauftragnehmer, Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten oder mit ihnen in Berührung kommen können.

(bitte wählen Sie einzelne auf Sie zutreffenden Maßnahmen durch Anklicken aus)

- ☐ Darüber hinaus beruht die Auftragsverarbeitung im Einzelnen auf dem Vertrag

\_\_\_\_\_ vom \_\_\_\_\_ (Hauptvertrag).

- ☐ Ein dieser Vereinbarung zugrundeliegender Vertrag (Hauptvertrag) existiert nicht.

## 2. Gegenstand des Auftrags/der Verarbeitung

Der Auftragnehmer übernimmt folgende Verarbeitungen:

Beschreibung der Dienstleistungen im Rahmen des Vertrags

## 3. Dauer des Auftrags/der Verarbeitung

(bitte wählen Sie einzelne auf Sie zutreffende Maßnahmen durch Anklicken aus)

- ☐ Die Dauer/Laufzeit des Vertrags entspricht der Dauer des zugrundeliegenden Hauptvertrags.

- ☐ Die Dauer/Laufzeit des Vertrags ist befristet bis \_\_\_\_\_.

- ☐ Die Dauer/Laufzeit des Vertrags ist unbefristet und kann mit einer Frist von \_\_\_\_\_ von beiden Parteien gekündigt werden.

- ☐ Die Dauer/Laufzeit des Vertrags endet nach einmaliger Ausführung.

#### 4. Art und Zweck der Verarbeitung

(bitte wählen Sie einzelne auf Sie zutreffende Maßnahmen durch Anklicken aus)

- ☐ Art und Zweck der Verarbeitung personenbezogener Daten sind im zugrundeliegenden Hauptvertrag konkret beschrieben.
- ☐ Konkretisierung der Beschreibung der Verarbeitungen/Dienstleistungen des Auftragnehmers im Hinblick auf Art und Zweck der Verarbeitung:

Nähere Beschreibung des Auftragsgegenstands/der Verarbeitungen und des Zwecks der Verarbeitung (Verarbeitungstätigkeit/en)

##### 4.1. Art der personenbezogenen Daten

s. Übersicht personenbezogene Daten <http://bit.ly/dsgvo-01>  
als Anlage 1 zu diesem Vertrag

##### 4.2. Kategorien betroffener Personen

s. Übersicht personenbezogene Daten <http://bit.ly/dsgvo-01>  
als Anlage 1.1 zu diesem Vertrag

#### 5. Anwendungsbereich und Verantwortlichkeit

- 5.1. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die ggfs. im Hauptvertrag und in der Leistungsbeschreibung 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 DSGVO).
- 5.2. Die Weisungen an den Auftragnehmer werden ggfs. durch den Hauptvertrag festgelegt und können darüber hinaus vom Auftraggeber in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Hauptvertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

## **6. Pflichten des Auftragnehmers**

- 6.1.** Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DSGVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.
- 6.2.** 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.
- 6.3.** Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DSGVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber und ggfs. Aufsichtsbehörden gegenüber sind diese technischen und organisatorischen Maßnahmen auf Anfrage nachzuweisen. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative, nachweislich adäquate Maßnahmen umzusetzen. Dabei muss sichergestellt sein, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren.

Eine Darstellung dieser technischen und organisatorischen Maßnahmen erfolgt in Anlage 2 zu diesem Vertrag. (s. Mustervorlage <http://bit.ly/dsgvo-04>)

- 6.4.** Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 d) DSGVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.
- 6.5.** Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Rechte betroffener Personen gem. Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen.
- 6.6.** Der Auftragnehmer selbst führt für die Verarbeitung ein Verzeichnis der bei ihm stattfindenden Verarbeitungstätigkeiten im Sinne des Art. 30 DSGVO. Er stellt auf Anforderung dem Auftraggeber die für die Übersicht nach Art. 30 DSGVO notwendigen Angaben zur Verfügung.
- 6.7.** Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort (Art. 28 Abs. 3 b) DSGVO).

- 6.8.** Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit.
- 6.9.** (bitte wählen Sie einzelne auf Sie zutreffende Maßnahmen durch Anklicken aus)
- ☐ Als Datenschutzbeauftragter ist beim Auftragnehmer derzeit
- [Name, Kontaktdaten]  
benannt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich schriftlich mitzuteilen. Der Auftragnehmer gewährleistet, dass die Anforderungen an den Datenschutzbeauftragten und seine Tätigkeit gemäß Art. 38 DSGVO erfüllt werden.
- ☐ Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird
- [Name, Kontaktdaten]  
benannt.
- ☐ Da der Auftragnehmer seinen Sitz außerhalb der Union hat, benennt er folgenden Vertreter nach Art. 27 Abs. 1 DSGVO in der Union:
- [Name, Kontaktdaten]
- 6.10.** 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.
- 6.11.** Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
- 6.12.** Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.
- 6.13.** Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 h) DSGVO).
- 6.14.** Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

- 6.15.** Der Auftragnehmer hat dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nachzuweisen. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch:

(bitte wählen Sie einzelne auf Sie zutreffende Maßnahmen durch Anklicken aus)

- ☐ die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO
- ☐ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO
- ☐ 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).

## 7. Pflichten des Auftraggebers

- 7.1.** Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.
- 7.2.** Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
- 7.3.** 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.

## 8. Subunternehmer (weitere Auftragsverarbeiter)

- 8.1.** Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.
- 8.2.** Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.
- 8.3.** (bitte wählen Sie einzelne auf Sie zutreffenden Maßnahmen durch Anklicken aus)

- ☐ Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung folgender Subunternehmer durchgeführt:  
**als Anlage 3 zu diesem Vertrag**

Name, Anschrift	Beschreibung der Teilleistungen
.....	.....
.....	.....

Vor der Hinzuziehung weiterer oder der Ersetzung aufgeführter Subunternehmer holt der Auftragnehmer die Zustimmung des Auftraggebers ein, wobei diese nicht ohne wichtigen datenschutzrechtlichen Grund verweigert werden darf.

- ☐ Eine Weitergabe von Aufträgen im Rahmen der in dem Vertrag vereinbarten Tätigkeiten an Subunternehmer durch den Auftragnehmer erfolgt nicht.

- 8.4.** Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.
- 8.5.** Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).
- 8.6.** Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.
- 8.7.** Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DSGVO bezüglich seiner Beschäftigten erfüllt hat.

## **9. Informationspflichten, Schriftformklausel, Rechtswahl**

- 9.1.** Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher« im Sinne der Datenschutz-Grundverordnung liegen.
- 9.2.** Änderungen und Ergänzungen dieses Vertrags und aller seiner Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
- 9.3.** Es gilt deutsches Recht.

## **10. Haftung und Schadensersatz**

- 10.1.** Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

Hier können weitere individuelle Vereinbarungen zwischen den Parteien getroffen werden.

## **11. Salvatorische Klausel**

- 11.1.** Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen der Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, bleiben die übrigen Vertragsbestimmungen und die Wirksamkeit des Vertrages im Ganzen hiervon unberührt.
- 11.2.** An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.
- 11.3.** Erweist sich der Vertrag als lückenhaft, gelten die Bestimmungen als vereinbart, die dem Sinn und Zweck des Vertrages entsprechen und im Falle des Bedachtwerdens vereinbart worden wären.

**Auftraggeber**

\_\_\_\_\_  
Ort, Datum

\_\_\_\_\_  
Unterschrift

**Auftragnehmer**

\_\_\_\_\_  
Ort, Datum

\_\_\_\_\_  
Unterschrift