# Vertrag zur Auftragsverarbeitung gemäss Art. 28 DSGVO

Dieser Vertrag zur Auftragsverarbeitung wird abgeschlossen zwischen

*[Eintragen: Firmenwortlaut und Anschrift des Verantwortlichen]*

(im Folgenden „Verantwortlicher“)

und

*[Eintragen: Firmenwortlaut und Anschrift des Auftragsverarbeiters]*

(im Folgenden „Auftragsverarbeiter“)

Der Auftragsverarbeiter verpflichtet sich, die im Folgenden beschriebenen Datenverarbeitungen im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO im Auftrag des Verantwortlichen zu erbringen. Für die Zwecke dieses Vertrages gelten die Begriffsbestimmungen der Datenschutz-Grundverordnung (DSGVO, Verordnung (EU) 2016/679).

## Gegenstand und Dauer des Vertrages

### Gegenstand

Der Auftrag umfasst Folgendes:

*(Gegenstand des Auftrags, konkrete Beschreibung der Dienstleistungen)*

### Dauer

Der Vertrag beginnt am .................................... und endet am ................................................

oder

Der Vertrag wird auf unbestimmte Zeit abgeschlossen und kann von beiden Parteien mit einer Frist von ...... *[Kündigungsfrist eintragen, z.B. ein Monat]* zum ....... *[Kündigungstermin eintragen, z.B. Kalendervierteljahr]* gekündigt werden.

Der Verantwortliche kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoss des Auftragsverarbeiters gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragsverarbeiter eine Weisung des Verantwortlichen nicht ausführen kann oder will oder der Auftragsverarbeiter Kontrollrechte des Verantwortlichen vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoss dar.

## Ort der Durchführung, Kategorien der personenbezogenen Daten, Kategorien betroffener Personen, Art und Zweck der Verarbeitung

|  |
| --- |
| Ort der Durchführung der AuftragsverarbeitungAlle Datenverarbeitungstätigkeiten werden ausschliesslich innerhalb der EU bzw. des EWR durchgeführt.Alternativ: Datenverarbeitungstätigkeiten werden zumindest zum Teil auch ausserhalb der EU bzw. des EWR durchgeführt, und zwar in ..... *[Staaten aufzählen]*. Das angemessene Datenschutzniveau ergibt sich aus *[alternativ, Nichtzutreffendes bitte streichen]*: * Einem Angemessenheitsbeschluss der Europäischen Kommission nach Art. 45 DSGVO.
* Einer Ausnahme für den bestimmten Fall nach Art. 49 Abs. 1 DSGVO.
* Verbindlichen internen Datenschutzvorschriften nach Art. 47 iVm Art. 46 Abs. 2 Bst. b DSGVO.
* Standarddatenschutzklauseln nach Art. 46 Abs. 2 Bst. c und d DSGVO.
* Genehmigten Verhaltensregeln nach Art. 46 Abs. 2 Bst. e iVm Art. 40 DSGVO.
* Einem genehmigten Zertifizierungsmechanismus nach Art. 46 Abs. 2 Bst. f iVm Art. 42 DSGVO.
* Von der Datenschutzbehörde bewilligten Vertragsklauseln nach Art. 46 Abs. 3 Bst. a DSGVO.
* einer Ausnahme für den Einzelfall nach Art. 49 Abs. 1 Unterabsatz 2 DSGVO.

Kategorien von Daten in Entsprechung von Art. 4 Nr. 1 DSGVODie übermittelten personenbezogenen Daten gehören zu folgenden Datenkategorien (bitte genau angeben): |

|  |
| --- |
| optional: Kategorien von sensiblen Daten in Entsprechung von Art. 4 Nr. 13, 14 und 15 DSGVODie übermittelten personenbezogenen Daten umfassen folgende sensible Daten: |
| Kategorien betroffener PersonenDie übermittelten personenbezogenen Daten betreffen folgende Kategorien betroffener Personen: |
| Art der Verarbeitung in Entsprechung von Art. 4 Nr. 2 DSGVODie übermittelten personenbezogenen Daten werden folgenden grundlegenden Verar­beitungsmassnahmen unterzogen: |
| VerarbeitungszweckeDie übermittelten personenbezogenen Daten werden zu folgenden vom Verantwortlichen bestimmten Zwecken verarbeitet: |

## Pflichten des Auftragsverarbeiters

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschliesslich gemäss den vertraglichen Bestimmungen dieses Vertrages oder wie vom Verantwortlichen in dokumentierter Weise angewiesen, es sei denn, der Auftragsverarbeiter ist gesetzlich zu einer weiteren Verarbeitung verpflichtet. Der Auftragsverarbeiter teilt solche Pflichten dem Verantwortlichen vor der Verarbeitung mit, es sei denn, das betreffende Recht verbietet eine solche Mitteilung wegen eines wichtigen öffentlichen Interesses (Art. 28 Abs. 3 Satz 2 Bst. a DSGVO).
2. Die unbedingte Befolgung der Anweisungen des Verantwortlichen gilt insbesondere auch in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder eine internationale Organisation – sofern der Auftragsverarbeiter nicht durch das Recht der Union oder des Mitgliedstaates, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.
3. Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Verantwortlichen in Folge in schriftlicher Form oder in einem elektronischen Format (Textform) an den Auftragsverarbeiter durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung).
4. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.
5. Der Auftragsverarbeiter verwendet die zur Verarbeitung überlassenen Daten für keine anderen Zwecke, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Zustimmung des Verantwortlichen nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.
6. Der Auftragsverarbeiter trennt die im Rahmen dieses Vertrages zu verarbeitenden Daten streng von anderen Datenbeständen.
7. Der Auftragsverarbeiter verpflichtet sich im Rahmen der Datenverarbeitung die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften zu beachten. Der Auftragsverarbeiter bestätigt, dass den von ihm zur Datenverarbeitung eingesetzten Personen die relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut sind. Entsprechende Schulungs- und Sensibilisierungsmassnahmen haben in regelmässigen Abständen zu erfolgen.
8. Der Auftragsverarbeiter erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragsverarbeiter aufrecht.
9. Optional: Er verpflichtet sich, auch folgende für diesen Auftrag relevanten Verschwiegenheitspflichten zu beachten, die dem Verantwortlichen obliegen: *.......................................................(z.B. Bankgeheimnis, Berufsgeheimnisse, etc.)*
10. Der Auftragsverarbeiter unterstützt den Verantwortlichen im erforderlichen Ausmass bei der Gewährung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO. Falls eine betroffene Person eine Anfrage direkt an den Auftragsverarbeiter sendet, leitet dieser die Anfrage umgehend an den Verantwortlichen weiter. Auskünfte an Dritte oder Betroffene darf der Auftragsverarbeiter nur nach vorheriger Zustimmung durch den Verantwortlichen erteilen.
11. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmassnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgenabschätzung, vorherige Konsultation).
12. Wird der Verantwortliche durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen, verpflichtet sich der Auftragsverarbeiter, den Verantwortlichen im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.
13. Der Auftragsverarbeiter informiert den Verantwortlichen umgehend, wenn eine erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstösst. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftragsverarbeiter nach Überprüfung bestätigt oder geändert wird.
14. Der Auftragsverarbeiter hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Verantwortliche dies verlangt und keine berechtigten Interessen des Auftragsverarbeiters dem entgegenstehen.
15. Gemäss Art. 37 DSGVO wurde Herr/Frau.............................................. *[Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail]* vom Auftragsverarbeiter als Datenschutzbeauftragter ernannt. Änderungen in der Person des Datenschutz­beauftragten teilt der Auftragsverarbeiter dem Verantwortlichen umgehend mit.

Oder: Ein betrieblicher Datenschutzbeauftragter ist beim Auftragsverarbeiter nicht bestellt, da die gesetzliche Notwendigkeit für eine Bestellung nicht vorliegt. Als Ansprechpartner für Datenschutzfragen beim Auftragsverarbeiter wird Herr/Frau [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail] benannt.

1. Optional: Da der Auftragsverarbeiter nicht im EWR niedergelassen ist, wird .............................................. *[Eintragen: Name, Organisation, Telefon, E-Mail]* als verantwortlicher Ansprechpartner („Vertreter“) im EWR gem. Art. 27 DSGVO bestellt. Änderungen in der Person des Vertreters werden dem Verantwortlichen umgehend mitgeteilt.

## Unterauftragsverarbeiter (Art. 28 Abs. 2 DSGVO, Art. 28 Abs. 3 Satz 2 Bst. d DSGVO)

Variante 1

1. Die Beauftragung von Unterauftragsverarbeitern durch den Auftragsverarbeiter ist nur mit Genehmigung des Verantwortlichen im Einzelfall gestattet.
2. Der Verantwortliche stimmt zu, dass die im Anhang ...... aufgelisteten Unterauftragsverarbeiter für den Auftragsverarbeiter tätig sind. Die Art und der Umfang ihrer Datenverarbeitung sind ebenfalls in Anhang ..... definiert.
3. Die vertraglich vereinbarten Regelungen zwischen Verantwortlichem und Auftragsverarbeiter gelten auch gegenüber Unterauftragsverarbeitern.
4. Dem Verantwortlichen ist auf Anfrage Einsicht in die relevanten Verträge zwischen dem Auftragsverarbeiter und dem Unterauftragsverarbeiter zu gewähren.
5. Der Verantwortliche ist berechtigt, jederzeit in dem hier festgelegten Umfang Kontrollen auch bei Unterauftragsverarbeitern durchzuführen oder durch Dritte durchführen zu lassen.
6. Die Verantwortlichkeiten des Auftragsverarbeiters und Unterauftragsverarbeiters sind klar voneinander abzugrenzen.
7. Kommt der Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Unterauftragsverarbeiters.

Variante 2:

1. Der Auftragsverarbeiter ist befugt, jederzeit Unterauftragsverarbeiter zu beauftragen.
2. Die Beauftragung ist dem Verantwortlichen vor der Auftragsvergabe anzuzeigen.
3. Der Verantwortliche hat gemäss Art. 28 Abs. 2 DSGVO ein Recht auf Einspruch gegen diese Beauftragung.
4. Im Falle eines Einspruches ...... (Da die DSGVO die Folgen dieses Einspruchs nicht regelt, wird empfohlen, diese vertraglich festzulegen. Wird keine Regelung getroffen, ist die Bestellung des Unterauftragsverarbeiters, gegen den Einspruch erhoben wurde, nicht möglich.)
5. Die Punkte 3-7 in Variante 1 gelten auch bei Wahl der Variante 2.

Variante 3:

Der Auftragsverarbeiter ist nicht berechtigt, einen Unterauftragsverarbeiter zu beauftragen.

## Technische und organisatorische Massnahmen

1. Der Auftragsverarbeiter ergreift alle erforderlichen Massnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art. 32 DSGVO. Die Massnahmen gewährleisten ein dem Risiko angemessenes Schutzniveau hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.
2. Die erforderlichen technischen und organisatorischen Massnahmen sind im Anhang ..... zu diesem Vertrag dokumentiert.
3. Wesentliche Änderungen sind ebenfalls umgehend zu dokumentieren.
4. Soweit die getroffenen Sicherheitsmassnahmen den Anforderungen des Verantwortlichen nicht oder nicht mehr genügen, benachrichtigt Letzterer den Auftragsverarbeiter.

## Verpflichtungen des Auftragsverarbeiters nach Beendigung des Auftrags (Art. 28 Abs. 3 Satz 2 Bst. g DSGVO)

1. Der Auftragsverarbeiter ist nach Beendigung der Auftragsverarbeitung verpflichtet, alle Verarbeitungsergebnisse und übermittelten personenbezogenen Daten und deren Kopien, dem Verantwortlichen zurückzugeben [bzw. alternativ] in dessen Auftrag zu vernichten, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Die Rückgabe der Kopien bzw. der Abschluss des Löschvorgangs ist schriftlich zu bestätigen.
2. Wenn der Auftragsverarbeiter die Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die Daten nach Beendigung dieser Vereinbarung entweder in diesem Format oder nach Wunsch des Verantwortlichen in dem Format, in dem er die Daten vom Verantwortlichen erhalten hat oder in einem anderen, gängigen Format zurückzugeben.

## Rechte und Pflichten des Verantwortlichen

**Der Verantwortliche ist berechtigt,**

1. die Einhaltung der vom Auftragsverarbeiter getroffenen technischen und organisatorischen Massnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen in angemessenem Umfang selbst oder durch Dritte vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragsverarbeiter soweit erforderlich Zutritt und Einblick zu ermöglichen. Der Auftragsverarbeiter erteilt die erforderlichen Auskünfte.
2. Kontrollen beim Auftragsverarbeiter erfolgen ohne vermeidbare Störungen seines Geschäftsbetriebs und ausser bei dringlichen Gründen nach angemessener Vorankündigung und während der Geschäftszeiten des Auftragsverarbeiters.

**Der Verantwortliche ist verpflichtet:**

1. sicher zu stellen, dass die Rechtmässigkeit der Verarbeitung gemäss Art. 6 Abs. 1 bzw. Art. 9 Abs. 2 DSGVO gegeben ist;
2. zu gewährleisten, dass die Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO gewahrt werden. Wenn allerdings nur der Auftragsverarbeiter die Kompetenz hat, den Anfragen nachzukommen, leitet der Verantwortliche ihm die betreffenden Anfragen umgehend weiter;
3. dem Auftragsverarbeiter Aufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format zu übermitteln. Mündliche Weisungen sind schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen;
4. den Auftragsverarbeiter unverzüglich über Fehler oder Unregelmässigkeiten bei der Prüfung der Auftragsergebnisse zu informieren;
5. alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmassnahmen des Auftragsverarbeiters vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

## Haftung

Es wird auf Art. 82 DSGVO verwiesen.

Alternativ: Eigene Vereinbarung zwischen den Parteien.

## Sonstiges

Individuell zu ergänzen

**Unterschriften**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| Ort, Datum | Ort, Datum |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| Verantwortlicher | Auftragsverarbeiter |

**Alle zu treffenden Massnahmen sind vertraglich konkret zu bestimmen - pauschale Aussagen und Wiederholungen der gesetzlichen Vorschriften genügen hierfür nicht.**

**Nachfolgend finden Sie Erläuterungen und Beispiele zu den gesetzlich vorgeschriebenen Massnahmen. Präzisieren Sie diese entsprechend den Gegebenheiten in Ihrer Organisation!**

## 1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

* **Zutrittskontrolle**
Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;
* **Zugangskontrolle**
Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
* **Zugriffskontrolle**
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;
* **Trennungskontrolle**
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;
* **Pseudonymisierung** (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)
Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Massnahmen unterliegen.

## 2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

* **Weitergabekontrolle**
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur
* **Eingabekontrolle**
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungs­systeme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement.

## 3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

* **Verfügbarkeitskontrolle**
Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;
* Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO).

## 4. Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

* Datenschutz-Management;
* Incident-Response-Management;
* Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);
* Auftragskontrolle
Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Verantwortlichen, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungs­pflicht, Nachkontrollen.