# **Anwendungsbeispiel für einen Vertrag zur Auftragsverarbeitung**

# **gemäß Art. 28 DS-GVO**

|  |
| --- |
| **Dieses Anwendungsbeispiel soll zur Unterstützung bei der Ausgestaltung der Auftragsverarbeitung nach Art. 28 DS-GVO dienen. Es stellt keine Standardvertragsklausel nach Art. 28 Abs. 7 und 8 DS-GVO dar und erhebt nicht den Anspruch einer vollständigen und abschließenden Regelung zu Art. 28 DS-GVO.** |

**Vertrag**

zwischen dem/der

|  |
| --- |
| *(Verantwortlichen)* |

- nachstehend Auftraggeber genannt -

und dem/der

|  |
| --- |
| *(Auftragsverarbeiter/in)* |

- nachstehend Auftragnehmer genannt -

## **1. Gegenstand und Dauer des Vertrages**

(1) Gegenstand des Vertrages

* Der Gegenstand des Vertrages ist die Verarbeitung von personenbezogenen Daten des Auftragnehmers für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieses Vertrages.

Die Verarbeitung umfasst folgende Arbeiten:

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

*(Definition der Datenverarbeitung)*

*Beispiele:*

• *Vernichtung von dienstlichem Schriftgut mit personenbezogenen Daten*

• *Wartung und Fernwartung von IT-Technik, sofern der Zugang zu personenbezogenen*

*Daten nicht ausgeschlossen ist*

• *Bewachungsdienstleistung, die die Verarbeitung personenbezogener Daten umfasst wie z.B. Wachschutz mit Videoüberwachung*

• *Übernahme von Rechnerleistungen durch ein Rechenzentrum*

*(Weitere Beispiele können dem Kurzpapier Nr. 13 der Datenschutzkonferenz entnommen werden.)*

*oder*

* Der Gegenstand des Vertrages ist die Verarbeitung von personenbezogenen Daten des Auftragnehmers für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieses Vertrages und ergibt sich aus der Leistungsvereinbarung/SLA/................................................. vom ..................., auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung).

(2) Dauer des Vertrages

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

*oder*

* Die Dauer dieses Vertrages (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

*oder*

Der Vertrag wird zur einmaligen Ausführung erteilt.

*oder*

* Der Vertrag wird auf unbestimmte Zeit geschlossen. Er kann von beiden Parteien mit einer

Frist von ................... zum ................... gekündigt werden.

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

## **2. Art und Zweck der Verarbeitung**

* Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung vom ...................

*oder*

* Art und Zweck der Verarbeitung sind:

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

*(nähere Beschreibung entsprechend der Definition von Art. 4 Nr. 2 DS-GVO)*

Die vertraglich vereinbarte Datenverarbeitung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Datenverarbeitung oder Teilarbeiten davon 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 ………………………. *(Drittland).*

* ist festgestellt durch einen Angemessenheitsbeschluss der Kommission

(Art. 45 Abs. 3 DS-GVO);

* wird hergestellt durch verbindliche interne Datenschutzvorschriften

(Art. 46 Abs. 2 lit. b i.V.m. 47 DS-GVO);

* wird hergestellt durch Standarddatenschutzklauseln

(Art. 46 Abs. 2 lit. c und d DS-GVO);

* wird hergestellt durch genehmigte Verhaltensregeln

(Art 46 Abs. 2 lit. e i.V.m. 40 DS-GVO);

* wird hergestellt durch einen genehmigten Zertifizierungsmechanismus

(Art. 46 Abs. 2 lit. f i.V.m. 42 DS-GVO).

* wird hergestellt durch sonstige Maßnahmen: …………………………….

(Art. 46 Abs. 2 lit. a, Abs. 3 lit. a und b DS-GVO).

## **3. Art der personenbezogenen Daten und Kategorien betroffener Personen**

(1) Art der personenbezogenen Daten

* Die Art der personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben unter: .......................

*oder*

* Gegenstand der Verarbeitung sind folgende personenbezogene Daten: *(Aufzählung/Beschreibung der Datenkategorien entsprechend der Definition von Art. 4 Nr. 1 DS- GVO):*
* Personenstammdaten (z.B. Name, Anschrift)
* Kommunikationsdaten/ Kontaktdaten (z.B. Telefon, E-Mail)
* Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
* Kundenhistorie
* Vertragsabrechnungs- und Zahlungsdaten
* Planungs- und Steuerungsdaten
* Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
* Daten nach Art. 9 DS-GVO
* …

(2) Kategorien betroffener Personen

* Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der Leistungsvereinbarung konkret beschrieben unter: ..................................

*oder*

* Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:
* Kunden
* Interessenten
* Abonnenten
* Beschäftigte
* Lieferanten
* Handelsvertreter
* Ansprechpartner
* ...

**4. Allgemeine Pflichten von Auftragnehmer und Auftraggeber**

(1) 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 ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

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

(3) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung besteht nach Beendigung dieses Vertrages fort.

(4) Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind. Er verpflichtet sich, auch folgende für diesen Auftrag relevanten Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen:

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

(z. B. Bankgeheimnis, Fernmeldegeheimnis, Sozialgeheimnis, Berufsgeheimnisse nach § 203 StGB etc.)

**5. Weisungsbefugnis des Auftraggebers und Weisungsempfänger des Auftragnehmers**

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

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen die DS-GVO oder andere Datenschutzbestimmungen (Art. 28 Abs. 3 S. 3 DS-GVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber geprüft und im Anschluss bestätigt oder geändert wird.

(3) Weisungsberechtigte Personen des Auftraggebers sind:

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

(Vorname, Name, Organisationseinheit, Telefon, E-Mail)

Weisungsempfänger beim Auftragnehmer sind:

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

(Vorname, Name, Organisationseinheit, Telefon, E-Mail)

Für Weisungen zu nutzende Kommunikationskanäle:

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

(postalische Adresse/ E-Mail/ Telefonnummer)

(4) Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

**6. Mitteilungs- und Unterstützungspflichten von Auftragnehmer und Auftraggeber**

(1) 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. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DS-GVO. Meldungen nach Art. 33 oder 34 DS-GVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gemäß Ziffer 5 dieses Vertrages durchführen.

(2) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, bei der Erfüllung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO, bei Meldepflichten bei Datenpannen, bei der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten, bei Datenschutz-Folgeabschätzungen und vorherigen Konsultationen. Hierzu gehören u.a.

* die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
* die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
* die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
* die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
* die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

(3) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

*(4) Sofern einschlägig:* Der Auftragnehmer verpflichtet sich, den Auftraggeber über den Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DS-GVO und den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 DS-GVO unverzüglich zu informieren.

**7. Datenschutzbeauftragte/r und Beschäftigte des Auftragnehmers**

(1) Beauftragte/r für den Datenschutz

* Beim Auftragnehmer ist folgende/r Beauftragte/r für den Datenschutz bestellt, der/die seine/ihre Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt:

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

(Vorname, Name, Organisationseinheit, Telefon, E-Mail)

Ein Wechsel des/der Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

*oder*

* Beim Auftragnehmer ist ein/e Beauftragte/r für den Datenschutz bestellt, der/die seine/ihre Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Ein Wechsel des/der Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen. Die jeweils aktuellen Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt *oder* werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt.

*oder*

* Der Auftragnehmer ist nicht zur Bestellung eines/einer Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Herr/Frau *(Vorname, Name, Organisationseinheit, Telefon, E-Mail)* benannt.

*oder*

* Da der Auftragnehmer seinen Sitz außerhalb der Union hat, benennt er folgenden Vertreter nach Art. 27 Abs. 1 DS-GVO in der Union: (*Vorname, Name, Organisationseinheit, Telefon, E-Mail).*

(2) Beschäftigte beim Auftragnehmer

Zur Wahrung der Vertraulichkeit (Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO) setzt der Auftragnehmer bei der Durchführung der Arbeiten nur Beschäftigte ein, die vor Aufnahme ihrer Tätigkeit auf die Vertraulichkeit, die sie während und nach Beendigung des Beschäftigungsverhältnisses zu wahren haben, verpflichtet wurden. Sie sind mit den für sie relevanten Bestimmungen zum Datenschutz vertraut zu machen.

Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) ist nur mit Zustimmung des Auftraggebers gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist vorher der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers vertraglich sicher zu stellen. Die Maßnahmen nach Art. 32 DS-GVO sind auch in diesem Fall sicherzustellen.

**8. Kontrollrechte des Auftraggebers**

(1) Der Auftraggeber hat das Recht vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise, im Benehmen mit dem Auftragnehmer - grundsätzlich nach Terminvereinbarung - Überprüfungen durchzuführen oder durch vom Auftraggeber beauftragte Dritte durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieses Vertrages sowie der Vorschriften über Datenschutz und Datensicherheit durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Die Kontrollen umfassen insbesondere die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO). Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt, dem Auftraggeber die erforderlichen Auskünfte erteilt und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachweist.

(3) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

(4) Der Auftragnehmer hat über die gesamte Abwicklung der Dienstleistung für den Auftraggeber insbesondere folgende Überprüfungen in seinem Bereich durchzuführen:

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

Das Ergebnis der Kontrollen ist zu dokumentieren.

**9. Kontrollen der Aufsichtsbehörde**

(1) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

(2) Der Auftraggeber informiert den Auftragnehmer unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

(3) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer soweit möglich zu unterstützen.

**10. Unterauftragsverhältnisse**

(1) Die Beauftragung von Subunternehmern (weitere Auftragsverarbeiter) zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 DS-GVO:

* Eine Unterbeauftragung ist unzulässig.

*oder*

* Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu:

|  |  |  |
| --- | --- | --- |
| Unterauftragnehmer (Firma) | Anschrift/Land | Leistung |
|  |  |  |
|  |  |  |

* Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:
* der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
* der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
* eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(2) Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO).

(3) Der Auftragnehmer trägt dafür Sorge, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

(4) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/ Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer

* ist nicht gestattet;
* bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform) und der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform);

sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

(6) Eine Beauftragung von Subunternehmern zur Erbringung der vereinbarten Leistung in Drittstaaten (außerhalb der EU/des EWR) darf nur erfolgen, wenn der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicherstellt. Dazu müssen die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sein (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

(7) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet. Zur Datenweiterleitung müssen insbesondere die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt sein.

(8) Der Auftragnehmer hat die Einhaltung der Pflichten des/der Subunternehmer(s) wie folgt zu überprüfen:

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

Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen.

(9) Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

**11. Umgang mit personenbezogenen Daten**

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden). In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).

(2) Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen 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.

(3) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers und sofern berechtigte Interessen des Auftragnehmers nicht entgegenstehen, berichtigen, löschen oder deren Verarbeitung einschränken. Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

(4) Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(5) Der Auftragnehmer sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden. Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

(6) 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 bzw. zu löschen. Gleiches gilt für Test- und Ausschussmaterial. Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen. Das Protokoll der Löschung bzw. Vernichtung ist auf Anforderung vorzulegen.

(7) 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.

**12. Technische und organisatorische Maßnahmen**

(1) Der Auftragnehmer gewährleistet die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 32 DS-GVO (Art. 28 Abs. 3 S. 2 lit. c DS-GVO) *(Einzelheiten in Anlage 1)*. Er sorgt für die Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 8 dieses Vertrages.

(2) Bei den zu treffenden technischen und organisatorischen Maßnahmen handelt es sich, um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus 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 DS-GVO zu berücksichtigen.

(3) Das in der *Anlage 1* beschriebene Datenschutzkonzept stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach dem Stand der Technik hinreichend detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragnehmer dar.

(4) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(5) Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber abzustimmen. Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.

(6) Die technischen und organisatorischen Maßnahmen beim Auftragnehmer unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau bzw. die vereinbarten Standards der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

(7) Für die auftragsgemäße Verarbeitung personenbezogener Daten wird folgende Methodik zur Risikobewertung verwendet, welche die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten berücksichtigt:

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

(8) Das in der *Anlage 1* beschriebene Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der datenschutzkonformen Verarbeitung wird als verbindlich festgelegt.

(9) Der Nachweis von technischen und organisatorischen Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

* die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
* die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
* 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).

(10) Der Nachweis durch Zertifizierung nach Absatz 9 erfolgt durch:

* 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.

(11) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

**13. Vergütung**

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

**14. Haftung**

Auf Art. 82 DS-GVO wird verwiesen. Im Übrigen wird folgendes vereinbart:

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

**15. Vertragsstrafe**

Bei Verstoß des Auftragnehmers gegen die Regelungen dieses Vertrages, insbesondere zur Einhaltung des Datenschutzes, wird eine Vertragsstrafe von ................... Euro vereinbart.

**16. Sonstiges**

(1) Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

(2) Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich. *(optional)*

(3) Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz - oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen. *(optional)*

(4) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen. *(optional)*

**17. Wirksamkeit des Vertrages**

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

|  |  |  |
| --- | --- | --- |
| Ort, Datum |  | Ort, Datum |
| Unterschrift Auftraggeber |  | Unterschrift Auftragnehmer |

# **Anlage – Technische und organisatorische Maßnahmen**

# *(individuell anpassen)*

## **1. Pseudonymisierung und Verschlüsselung** **(Art. 32 Abs. 1 lit. a DS-GVO)**

* Pseudonymisierung  
  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 technischen und organisatorischen Maßnahmen unterliegen,
* Verschlüsselung

Vorgang, bei dem klar lesbare Informationen (Klartext) mit Hilfe eines Verschlüsselungsverfahrens (Kryptosystem) in eine nicht einfach interpretierbare Zeichenfolge (Geheimtexte) umgewandelt werden

## **2. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)**

* 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

## **3. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)**

* 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

## **4. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)**

* 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 DS-GVO);

## **5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung**

## **(Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)**

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