**Vertrag zur Auftragsverarbeitung**

Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag gem. Art. 28 DSGVO

zwischen

|  |
| --- |
| **IT-Systembetreuung Oliver Seidel** |

- nachstehend Auftraggeber genannt -

und

|  |
| --- |
|  |

- nachstehend Auftragnehmer genannt –

**Präambel**

Dieser Vertrag konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer beauftragte personenbezogene Daten des Auftraggebers verarbeitet werden.

**1. Gegenstand und Dauer des Auftrags**

***Gegenstand des Auftrags***

Der Gegenstand des Auftrags ergibt sich aus der Vereinbarung, auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung genannt):

|  |
| --- |
|  |

oder

Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: (Definition der Aufgaben)

|  |
| --- |
|  |
|  |

***Dauer des Auftrags***

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

oder (insbesondere, falls keine Leistungsvereinbarung zur Dauer besteht)

Der Auftrag wird zur einmaligen Ausführung erteilt.

oder

Die Dauer dieses Auftrags (Laufzeit) ist befristet bis \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

oder

Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ zum \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

**2. Konkretisierung des Auftragsinhalts**

***Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten***

Umfang, Art und Zweck der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung vom \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

oder

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Umfang, Art und Zweck der Aufgaben des Auftragnehmers:

|  |
| --- |
|  |
|  |
|  |

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

***Art der Daten***

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

|  |
| --- |
|  |

oder

Gegenstand der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten sind folgende Datenarten / -kategorien (Aufzählung / Beschreibung der Datenkategorien)

|  |  |  |
| --- | --- | --- |
| Adressdaten | Kontaktdaten | Vertragsdaten |
| Bankverbindungsdaten | Kontodaten | Abrechnungsdaten |
| Leistungsdaten | Finanzdaten | Angebotsdaten |
| Gesprächshistorie | Transaktionsdaten | Auskünfte |
| Mitarbeiterdaten | Personalverwaltung | Qualifikationsdaten |
| Videoaufzeichnungen | Gesundheitsdaten | Kundenhistorie |

Andere sensitive Daten:

|  |
| --- |
|  |

***Kreis der Betroffenen***

Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen ist in der Leistungsvereinbarung konkret beschrieben unter:

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

oder

|  |  |  |
| --- | --- | --- |
| Mitarbeiter | Ruheständler | Auszubildende |
| Praktikanten | Frühere Mitarbeiter | Bewerber |
| Unterhaltsberechtigte | Angehörige | Kunden |
| Interessenten | Lieferanten/Dienstleister | Berater |
| Makler | Vermittler | Mieter |
| Gesellschafter | Geschädigte | Zeugen |
| Kontaktpersonen | Pressevertreter | Ehrenamt |

Sonstige: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**3. Technisch-organisatorische Maßnahmen**

1. 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. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
2. Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen 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 DSGVO zu berücksichtigen,
3. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden.

**4. Sperrung und Löschung von Daten**

1. Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers 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.
2. Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

**5. Kontrollen und sonstige Pflichten des Auftragnehmers**

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

1. Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. 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.
2. Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO (Anlage 1).
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 nach besten Kräften zu unterstützen.
4. 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.

**6. Anfragen und Rechte Betroffener**

1. Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12-22 DSGVO.
2. Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist den Betroffenen unverzüglich an den Auftraggeber und warte dessen Weisungen ab.

**7. Unterauftragsverhältnisse**

1. Soweit bei der Verarbeitung oder Nutzung personenbezogener Daten des Auftraggebers Unterauftragnehmer einbezogen werden sollen, wird dies genehmigt, wenn folgende Voraussetzungen vorliegen:

* Ohne schriftliche Zustimmung kann der Auftragnehmer zur Vertragsdurchführung unter Wahrung seiner unter Punkt 5 erläuterten Pflicht zur Auftragskontrolle konzernangehörige Unternehmen sowie im Einzelfall andere Unterauftragnehmer mit der gesetzlich gebotenen Sorgfalt einsetzen, wenn er dies dem Auftraggeber vor Beginn der Verarbeitung oder Nutzung mitteilt.
* Der Auftragnehmer hat die vertraglichen Vereinbarungen mit dem / den Unterauftragnehmer/n so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen.

1. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.
2. Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.
3. Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO:

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

1. Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers ist 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.

**8. Kontrollrechte des Auftraggebers**

1. Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
2. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch:

* die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
* die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;

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

**9. Mitteilung bei Verstößen des Auftragnehmers**

1. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.
2. 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
3. die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
4. 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
5. Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

**10. Weisungsbefugnis des Auftraggebers**

1. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).
2. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

**11. Löschung von Daten und Rückgabe von Datenträgern**

1. 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.
2. 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.
3. 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.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ort, Datum |  | Unterschrift Auftragnehmer |  | Stempel |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ort, Datum |  | Unterschrift Auftraggeber |  | Stempel |

**Anlage 1: Allgemeine technische und organisatorische Maßnahmen**

**Vertraulichkeit Art. 32 Abs. 1 lit. b DSGVO**

**1. Zutrittskontrolle**

Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist. Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insb. auch zur Legitimation der Berechtigten:

Zutrittskontrollsystem, Ausweisleser, Magnetkarte, Chipkarte

Schlüssel/Schlüsselvergabe

Verwaltung der Zutrittsberechtigungen

Türsicherung (elektrische Türöffner usw.)

Sicherheitsschlösser

Werkschutz, Pförtner

Sorgfältige Auswahl von Reinigungsmaterial

Überwachungseinrichtung

Alarmanlage, Video-/Fernsehmonitor

**2. Zugangskontrolle**

Das Eindringen Unbefugter in die DV-Systeme ist zu verhindern.

Technische (Kennwort-/Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel)

Authentifikation mit Benutzername / Passwort

Einsatz von VPN-Technologien

Verschlüsselung von Smartphone-Inhalten

Automatische Sperrung (Pausenschaltung)

Einrichtung eines Benutzerstammsatzes pro User

Sperrung des Users nach Fehlversuchen

Zwei-Faktor-Authentifizierung

Verschlüsselung von Datenträgern

Einsatz von Anti-Viren-Software

Einsatz einer Firewall

**3. Zugriffskontrolle**

Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.

Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

Differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte)

Verwaltung der Rechte durch den Systemadministrator

Sichere Aufbewahrung von Datenträgern

Auswertungen

Kenntnisnahme

Veränderung

Verschlüsselungsverfahren

Löschung

Einsatz von Aktenvernichtern

Protokollierung der Vernichtung

**Integrität Art. 32 Abs. 1 lit. b DSGVO**

**4. Weitergabekontrolle**

Aspekte der Weitergabe personenbezogener Daten sind zu regeln: Elektronische Übertragung, Datentransport, Übermittlungskontrolle, Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:

Verschlüsselung/Tunnelverbindung (VPN)

Elektronische Signatur

Protokollierung

Transportsicherung

E-Mail-Verschlüsselung

**5. Eingabekontrolle**

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:

Protokollierungs- und Protokollauswertungssysteme

Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines

Berechtigungskonzepts

**6. Auftragskontrolle**

Die weisungsgemäße Auftragsdatenverarbeitung ist zu gewährleisten.

Maßnahmen (technisch / organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer:

Eindeutige Vertragsgestaltung

Formalisierte Auftragserteilung (Auftragsformular)

Kriterien zur Auswahl des Auftragnehmers

Kontrolle der Vertragsausführung

Vorgehensweise bei Vertragsbeendigung

**Verfügbarkeit und Belastbarkeit Art. 32 Abs. 1 lit. b DSGVO**

**7. Verfügbarkeitskontrolle**

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Maßnahmen zur Datensicherung (physikalisch/logisch):

Backup-Verfahren

Spiegeln von Festplatten, z.B. RAID-Verfahren

Unterbrechungsfreie Stromversorgung (USV)

Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

Virenschutz/Firewall

Notfallplan

Klimaanlage in Serverräumen

Test der Notfalleinrichtungen

Feuer- und Rauchmeldeanlagen

Feuerlöschgeräte in Serverräumen

**8. Trennungskontrolle**

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

Logische Mandantentrennung (softwareseitig)

physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern

Erstellung eines Berechtigungskonzepts

Festlegung von Datenbankrechten

Trennung von Produktiv- und Testsystem