Auftrags-verarbeitungsvertrag

NACH ART 28 DSGVO SOWIE MIT TECHNISCHEN-ORGANISATORISCHEN-MASSANAHMEN

[Auftraggeber]

nachfolgend «Auftraggeber» genannt

und

[Auftragnehmer]

nachfolgend «Auftragnehmer» genannt

gemeinsam nachfolgend als «Vertragspartner» genannt

1. Vertragsgegenstand

1.1. Gegenstand dieses Auftrages ist die Durchführung folgender Aufgaben: **[detaillierte Beschreibung der Aufgaben des Auftragnehmers, einschliesslich Art und Zweck der vorgesehenen Verarbeitung]**.

1.1.1. {Falls es einen weitergehenden Rahmenvertrag, Werkvertrag, Leistungsvereinbarung, gibt} Diese Vereinbarung ist als Ergänzung zu **[Vertrag von Datum]** zu verstehen.

1.2. Folgende Datenkategorien werden verarbeitet: **[Datenkategorien aufzählen, z.B. Kontaktdaten, Vertragsdaten, Verrechnungsdaten, Bonitätsdaten, Bestelldaten, Entgeltdaten, usw.]**.

2. Dauer der Vereinbarung

2.1. {Einmalige Durchführung} Die Vereinbarung endet mit einmaliger Durchführung der Arbeiten.

{Befristete Laufzeit} Die Vereinbarung ist befristet abgeschlossen und endet mit **[Fristende eintragen]**.

{Unbefristete Laufzeit} Die Vereinbarung ist auf unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist von **[Kündigungsfrist eintragen]** zum **[Kündigungstermin eintragen]** gekündigt werden. Die Möglichkeit zur ausserordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

3. Pflichten des Auftragnehmers

3.1. Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschliesslich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er - sofern gesetzlich zulässig - den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragnehmers eines schriftlichen Auftrages.

3.2. Der Auftragnehmer 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 Auftragnehmer aufrecht.

3.3. Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Massnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat **[Einzelheiten sind der Anlage 1 zu entnehmen]**.

3.4. Der Auftragnehmer ergreift die technischen und organisatorischen Massnahmen, damit der Auftraggeber die Rechte der betroffenen Person nach Kapitel III der DSGVO

(Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenverarbeitung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.

3.5. Der Auftragnehmer unterstützt den Auftraggeber 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-Folgeabschätzung, vorherige Konsultation).

3.6. Der Auftragnehmer wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten hat.

3.7. Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch von ihm beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

3.8. Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu **[übergeben / in dessen Auftrag zu vernichten]**. Wenn der Auftragnehmer 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 Auftraggebers in dem Format, in dem er die Daten vom Auftraggeber erhalten hat oder in einem anderen, gängigen Format herauszugeben.

3.9. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstösst gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

4. Ort der Durchführung der Datenverarbeitung

4.1. {Ausschliessliche Durchführung innerhalb der EU/des EWR} Alle Datenverarbeitungstätigkeiten werden ausschliesslich innerhalb der EU bzw. des EWR durchgeführt.

{Bei Durchführung, wenn auch nur teilweise, ausserhalb der EU/des EWR} Datenverarbeitungstätigkeiten werden zumindest zum Teil auch ausserhalb der EU bzw. des EWR durchgeführt, und zwar in der Schweiz **[weitere Staaten aufzählen]**. Das angemessene Datenschutzniveau ergibt sich aus (zutreffendes ankreuzen):

☑ 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 lit b DSGVO.
☐ Standarddatenschutzklauseln
nach Art 46 Abs 2 lit c und d DSGVO.
☐ genehmigten Verhaltensregeln
nach Art 46 Abs 2 lit e iVm Art 40 DSGVO.
☐ einen genehmigten Zertifizierungsmechanismus
nach Art 46 Abs 2 lit f iVm Art 42 DSGVO.
☐ von der Datenschutzbehörde bewilligte Vertragsklauseln
nach Art 46 Abs 3 lit a DSGVO.
☐ einer Ausnahme für den Einzelfall
nach Art 49 Abs 1 Unterabsatz 2 DSGVO.

5. Sub-Auftragsverarbeiter

5.1. {Verbot der Hinzuziehung eines Sub-Auftragsverarbeiters} Der Auftragnehmer ist nicht berechtigt, einen Sub-Auftragsverarbeiter heranzuziehen.

{Zulässigkeit der Hinzuziehung eines bestimmten Sub-Auftragsverarbeiters} Der Auftragnehmer ist befugt folgendes Unternehmen als Sub-Auftragsverarbeiter hinzuziehen: **[Firmenname und Sitz ergänzen, Art der Tätigkeiten]**. Beabsichtigte Änderungen des Sub-Auftragsverarbeiters sind dem Auftraggeber so rechtzeitig schriftlich bekannt zu geben, dass er dies allenfalls untersagen kann. Der Auftragnehmer schliesst die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragnehmer auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

{Zulässigkeit der Hinzuziehung von Sub-Auftragsverarbeitern} Der Auftragnehmer kann Sub-Auftragsverarbeiter **[Tätigkeiten]** hinzuziehen. Er hat den Auftraggeber von der beabsichtigten Heranziehung eines Sub-Auftragsverarbeiters so rechtzeitig zu verständigen, dass er dies allenfalls untersagen kann. Der Auftragnehmer schliesst die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragnehmer auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

6. Schlussbestimmungen

6.1. Die Vertragspartner sind sich einig, dass der vorliegende Vertrag abschliessend ist und keine anderen auch mündliche Abreden getroffen wurden.

6.2. Änderungen und Ergänzungen der Vereinbarung bedürfen zu ihrer Wirksamkeit der Schriftform.

6.3. Erfüllungsort und Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit dieser Vereinbarung ist der Sitz des Beraters, sofern der Auftraggeber Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist.

6.4. Sollte eine Bestimmung dieser Vereinbarung ganz oder teilweise unwirksam sein oder werden oder sollte die Vereinbarung unvollständig sein, so wird die Vereinbarung im Übrigen Inhalt nicht berührt. Die Vertragspartner verpflichten sich, die unwirksame Bestimmung durch eine solche Bestimmung zu ersetzen, welche dem Sinn und Zweck der unwirksamen Bestimmung in rechtswirksamer Weise wirtschaftlich am nächsten kommt.

[Ort], den [Datum]	[Ort], den [Datum]
[Auftraggeber] [Firma]	[Auftragnehmer] [Firma]

Anlage 1
Technisch-Organisatorische Massnahmen

Vertraulichkeit

Zutrittskontrolle (Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen)

☐ Schlüssel	☐ Magnet- & Chipkarten
☐ Elektrische Türöffner	☐ Portier
☐ Sicherheitspersonal	☐ Alarmanlagen
☐ Videoanlage	☐ Einbruchshemmende Türe / Fenster
☐ Anmeldung beim Empfang mit Kontrolle	☐ Begleitung von Besuchern im Gebäude
☐ Tragen von Firmen- / Besucher-Ausweis	☐ Sonstiges:

Zugangskontrolle (Schutz vor unbefugter Systemnutzung)

☐ Kennwörter	☐ Verschlüsselung von Datenträgern
☐ Automatische Sperrmechanismen	☐ Zwei-Faktor-Authentifizierung
☐ Verschlüsselung von Datenleitungen	☐ Sonstiges:

Zugriffskontrolle (Kein unbefugtes Lesen, Verändern, Entfernen von Daten im System)

☐ Berechtigungsprofil auf «need to know»	☐ Prozess für Berechtigungsvergabe
☐ Protokollieren von Zugriffen	☐ Sichere Aufbewahrung von Datenträger
☐ Periodische Prüfung von Berechtigungen	☐ Clear-Desk / Clear-Screen-Policy
☐ Datenschutzgerechte Entsorgung von Datenträgern	☐ Datenschutzgerechte Wiederverwendung von Datenträgern
☐ Datenschutzgerechte Datensicherung	☐ Sonstiges:

Pseudonymisierung (Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenverarbeitung entfernt und gesondert aufbewahrt)

☐ Ja	☐ Nein

Klassifikation für Daten (Aufgrund gesetzlicher Verpflichtung oder Selbsteinschätzung (geheim / vertraulich / intern / öffentlich)

☐ Ja	☐ Nein

Datenintegrität

Weitergabekontrolle (Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport)

☐ Verschlüsselung von Datenträgern	☐ Verschlüsselung von Dateien
☐ Virtual Private Network (VPN)	☐ Elektronische Signatur
☐ Remote Desktop (RDP)	☐ Sonstiges:

Eingabekontrolle (Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind)

☐ Protokollierung	☐ Dokumentenmanagement
☐ One Time Passwort	☐ Sonstiges:

Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle (Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust)

☐ Backup-Strategie (Online / Offline)	☐ Unterbrechungsfreie Stromversorgung USV
☐ Virenschutz	☐ Firewall
☐ Meldewege und Notfallpläne	☐ Security Checks (Infrastruktur & Software)
☐ Mehrstufiges Sicherungskonzept (1)	☐ Standardprozess bei Mitarbeiterwechsel
☐ Infrastruktur-Massnahmen (1)	☐ Sonstiges:

1) = weitere Ausführungen siehe in separater Dokumentation

Wiederherstellbarkeit (Rasche Wiederherstellbarkeit in unter 15 Minuten möglich)

☐ Ja	☐ Nein

Verfahren zur regemässigen Überprüfung, Bewertung und Evaluierung

Datenschutz-Management

☐ Ja	☐ Nein

Incident-Response-Management

☐ Ja	☐ Nein

Datenschutzfreundliche Voreinstellungen

☐ Ja	☐ Nein

Auftragskontrolle (Auftragsdatenverarbeitung gemäss Art. 28 DSGVO auf Weisung des Auftraggebers)

☐ Eindeutige Vertragsgestaltung	☐ Formalisiertes Auftragsmanagement
☐ Strenge Auswahl des AV (ISO, ISMS o.ä.)	☐ Vorabüberzeugungspflicht

☐ Nachkontrollen	☐ Sonstiges: