

D_06a Auftragsverarbeitungsvertrag nach Art 28 DSGVO

abgeschlossen zwischen

[Name, Firma]
[Anschrift]
(Verantwortlicher)

nachstehend „Verantwortlicher“ genannt

einerseits

und

[Name, Firma]
[Anschrift]
(Auftragsverarbeiter)

nachstehend „Auftragsverarbeiter“ genannt

andererseits

wie folgt:

Präambel

Der Verantwortliche möchte den Auftragsverarbeiter mit den in Punkt 3. genannten Leistungen beauftragen. Teil der Vertragsdurchführung ist die Verarbeitung personenbezogener Daten. Insbesondere Art 28 DSGVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien die nachfolgende Vereinbarung.

1 Begriffsbestimmungen

Verantwortlicher ist gemäß Art 4 Z 7 DSGVO die Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Auftragsverarbeiter ist gemäß Art 4 Z 8 DSGVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Personenbezogene Daten sind gemäß Art 4 Z 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifiziert wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmal/en, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

Besonders schutzbedürftige personenbezogene Daten sind personenbezogene Daten gemäß Art 9 DSGVO, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugung oder die Gewerkschaftszugehörigkeit von Betroffenen hervorgehen, personenbezogene Daten gemäß Art 10 DSGVO über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen sowie genetische Daten gemäß Art 4 Z 13 DSGVO, biometrische Daten gemäß Art 4 Z 14 DSGVO, Gesundheitsdaten gemäß Art 4 Z 15 DSGVO sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Verarbeitung ist gemäß Art 4 Z 2 DSGVO jeder mit oder ohne Hilfe automatisiertes Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Aufsichtsbehörde ist gemäß Art 4 Z 21 DSGVO eine von einem Mitgliedstaat gemäß Art 51 DSGVO eingerichtete unabhängige staatliche Stelle (in Österreich die Datenschutzbehörde).

2 Gegenstand der Vereinbarung

- 2.1** Gegenstand dieses Auftrages ist die Durchführung folgender Aufgaben: *[möglichst detaillierte Beschreibung der Aufgaben des Auftragsverarbeiters, einschließlich Zweck der vorgesehenen Verarbeitung]*.
- 2.2** *[Falls es einen weitergehenden Rahmenvertrag, Werkvertrag, Leistungsvereinbarung, udgl gibt]* Diese Vereinbarung ist als Ergänzung zu *[Vertrag, etc samt Datum ergänzen]* zu verstehen.
- 2.3** Folgende Arten von personenbezogenen Daten werden verarbeitet: *[Datenkategorien aufzählen, zB Kontaktdaten, Vertragsdaten, Verrechnungsdaten, Bonitätsdaten, Bestelldaten, Entgeltdaten, usw.]*.
- 2.4** Folgende Kategorien betroffener Personen unterliegen der Verarbeitung: *[Betroffenenkategorien ergänzen, zB Kunden, Interessenten, Lieferanten, Ansprechpartner, Beschäftigte, usw.]*
- 2.5** Die Verarbeitung ist folgender Art: *[zB Erheben, Erfassen Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung von Daten]*

3 Dauer der Vereinbarung

- 3.1** *[Einmalige Durchführung]* Dieser Vertrag beginnt am *[Datum einfügen]* und endet nach einmaliger Ausführung.
- 3.2** *[Befristete Laufzeit]* Dieser Vertrag ist befristet abgeschlossen. Er beginnt mit *[Datum einfügen]* und endet mit *[Datum einfügen]*.
- 3.3** *[Unbefristete Laufzeit]* Die Vereinbarung ist auf unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist von *[Kündigungsfrist eintragen, zB ein Monat]* zum *[Kündigungstermin eintragen, zB Kalendervierteljahr]* gekündigt werden. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

4 Pflichten und Rechte des Auftragsverarbeiters

- 4.1** Der Auftragsverarbeiter verpflichtet sich, personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen – zu verarbeiten, sofern er nicht hierzu rechtlich verpflichtet ist. In solch einem Fall teilt der

Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern eine solche Mitteilung nicht rechtlich verboten ist.

- 4.2** 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.
- 4.3** Der Auftragsverarbeiter erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat (siehe Punkt 7 sowie Einzelheiten sind der **Anlage ./1¹** zu entnehmen).
- 4.4** Der Auftragsverarbeiter unterstützt angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen, damit der Verantwortliche seine Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen Person (zB Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Verantwortlichen alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Auftragsverarbeiter gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Verantwortlichen der von ihm betriebenen Datenanwendung hält, hat der Auftragsverarbeiter den Antrag unverzüglich an den Verantwortlichen weiterzuleiten und dies dem Antragsteller mitzuteilen.
- 4.5** Der Auftragsverarbeiter unterstützt unter Berücksichtigung der Art der Vereinbarung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (zB 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).
- 4.6** Der Auftragsverarbeiter hat für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten.
- 4.7** Dem Verantwortlichen wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch ihn beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt. Der Auftragsverarbeiter

¹ Anlage 1 (technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO) ist für das jeweilige Auftragsverarbeitungsverhältnis individuell zu erstellen.

verpflichtet sich, dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Vertrag niedergelegten Pflichten zur Verfügung stellt und Überprüfungen – einschließlich Inspektionen – die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, zu ermöglichen und dazu beizutragen.

- 4.8** Der Auftragsverarbeiter ist nach Beendigung dieser Vereinbarung verpflichtet – sofern nicht eine rechtliche Verpflichtung zur Speicherung besteht – alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Verantwortlichen **zu übergeben / in dessen Auftrag zu vernichten**.
- 4.9** Der Auftragsverarbeiter teilt dem Verantwortlichen unverzüglich Störungen, Verstöße des Auftragsverarbeiters 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. Meldungen nach Art. 33 oder 34 DSGVO für den Verantwortlichen darf der Auftragsverarbeiter nur nach vorheriger Weisung des Verantwortlichen durchführen.

5 Ort der Durchführung der Datenverarbeitung

Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw des EWR durchgeführt.

[ODER]

Datenverarbeitungstätigkeiten werden zumindest zum Teil auch außerhalb der EU bzw des EWR durchgeführt, und zwar in **[Staaten aufzählen]**. Das angemessene Datenschutzniveau ergibt sich aus **[nichtzutreffendes 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 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.

6 Sub-Auftragsverarbeiter

Der Auftragsverarbeiter ist nicht berechtigt, einen Sub-Auftragsverarbeiter hinzuzuziehen.

[ODER]

Der Auftragsverarbeiter ist befugt folgendes Unternehmen als Sub-Auftragsverarbeiter hinzuzuziehen: **[Firmenname und Sitz ergänzen, Art der Tätigkeiten]**. Beabsichtigte Änderungen des Sub-Auftragsverarbeiters sind dem Verantwortlichen so rechtzeitig schriftlich bekannt zu geben, dass er dies allenfalls untersagen kann. Der Auftragsverarbeiter schließt den erforderlichen Vertrag im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen einget, die dem Auftragsverarbeiter auf Grund dieses Vertrages obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art 44 ff DSGVO erfüllt sind (zB Angemessenheitsbeschluss der Kommission, genehmigte Verhaltensregeln).

Eine weitere Subbeauftragung durch den Subunternehmer ist (nicht) zulässig.

[ODER]

Der Auftragsverarbeiter kann Sub-Auftragsverarbeiter **[Tätigkeiten beschreiben]** hinzuziehen. Er hat den Verantwortlichen von der beabsichtigten Hinzuziehung eines Sub-Auftragsverarbeiters so rechtzeitig zu verständigen, dass er dies allenfalls untersagen kann. Der Auftragsverarbeiter schließt den erforderlichen Vertrag im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen einget, die dem Auftragsverarbeiter auf Grund dieses Vertrages obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art 44 ff DSGVO erfüllt sind (zB Angemessenheitsbeschluss der Kommission, genehmigte Verhaltensregeln).

Eine weitere Subbeauftragung durch den Subunternehmer ist (nicht) zulässig.

7 Technische und organisatorische Maßnahmen

- 7.1** Der Auftragsverarbeiter 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 DSGVO zu berücksichtigen [Einzelheiten in Anlage 1²].
- 7.2** Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und zuvor dem Verantwortlichen mitzuteilen.
- 7.3** Der Auftragsverarbeiter hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art 32 Abs 1 lit d DS-GVO). Das Ergebnis ist dem Verantwortlichen mitzuteilen.

8 Berichtigung, Einschränkung und Löschung von Daten

- 8.1** Der Auftragsverarbeiter darf die Daten, die aufgrund dieses Vertrages verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Verantwortlichen berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten.
- 8.2** Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Verantwortlichen unmittelbar durch den Auftragsverarbeiter sicherzustellen.

9 Haftung und Schadenersatz

Verantwortlicher und Auftragsverarbeiter haften gegenüber betroffenen Personen entsprechend der in Art 82 DSGVO getroffenen Regelungen.

² Anlage 1 (technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO) ist für das jeweilige Auftragsverarbeitungsverhältnis individuell zu erstellen.

10 Sonstiges

10.1 Änderungen und Ergänzungen dieses Vertrages – einschließlich etwaiger Zusicherungen des Auftragsverarbeiters – 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.

10.2 Sollten einzelne Bestimmungen dieses Vertrages unwirksam oder undurchführbar sein oder nach Vertragsschluss unwirksam oder undurchführbar werden, bleibt davon die Wirksamkeit des Vertrages im Übrigen unberührt.

10.3 Es gilt österreichisches Recht.

[Ort], am [Datum]

[Ort], am [Datum]

Für den Verantwortlichen:

Für den Auftragsverarbeiter:

.....
[Name samt Funktion]

.....
[Name samt Funktion]

Hinweis:

Dieses Muster dient der beispielsweise Umsetzung eines Auftragsverarbeitungsvertrages nach der DSGVO in Österreich für Mitglieder der WKO, Bundessparte Handel, und ist auf die Bedürfnisse des jeweiligen Unternehmens individuell anzupassen.

VERTRAG
nach Art 28 DSGVO

Seite **8** von **9**

Dieses Muster wurde mit größter Sorgfalt erstellt, für die Richtigkeit, Vollständigkeit, Aktualität oder Qualität des bereitgestellten Musters können wir jedoch keine Gewähr übernehmen. Haftungsansprüche gegen Personen, welche dieses Muster erstellt haben, sind daher ausgeschlossen.