Der Auftragsverarbeitungsvertrag

Wichtiger Hinweis

Dieser Mustervertrag ist auf eine „einfache“ Auftragsverarbeitung kleinerer und mittlerer Schweizer Unternehmungen im Anwedungsbereich des neuen Schweizer Bundesgesetzes über den Datenschutz[[1]](#footnote-1)   
(Art. 9 DSG) und der Europäischen Datenschutz-Grundverordnung[[2]](#footnote-2) (Art. 28 DSGVO) als Nachtrag oder Anhang zu einem Hauptvertrag zugeschnitten. Bei der praktischen Umsetzung ist jeweils auf den konkreten Anwendungsfall im Unternehmen abzustellen. Für die Auftragsverarbeitung in Drittländer, die keinen angemessenen Datenschutz gewährleisten, d.h. die meisten Länder ausserhalb des EWR und der Schweiz, müssen weitere geeignete Garantien vorgesehen werden. Als Option bieten sich beispielsweise die Standardvertragsklauseln der EU-Kommission[[3]](#footnote-3) auf Grundlage von Art. 46 Abs 2 lit. c DSGVO bzw. Art. 6 Abs. 2 lit. a DSG an.

Dieser Mustervertrag stellt eine unverbindliche, nicht abschliessende Vorlage für eine Auftragsverarbeitung nach Art. 28 DSGVO bzw. Art. 16 Abs. 2 lit. d. DSG dar. In der Vorlage wird soweit möglich auf die relevanten Bestimmungen beider Erlasse verwiesen. Für die Richtigkeit, Vollständigkeit und Aktualität des bereitgestellten Musters sowie auch für weiterführende Links kann aufgrund der derzeitigen Entwicklungen im Datenschutzrecht mit unterschiedlichen Anforderungen, Begriffsdefinitionen und Anwendungen sowohl in der EU, den Mitgliedstaaten des EWR (EU-Mitgliedstaaten einschliesslich Liechtenstein, Island, Norwegen) wie auch in der Schweiz sowie eines möglichen internationalen Bezugs der Verarbeitungstätigkeit keine Gewähr übernommen werden. Insbesondere bei komplexeren Auftragsverarbeitungen oder Verarbeitungen, die einen internationalen Bezug haben können, ist eine Zusammenarbeit mit einer Rechtsanwältin/einem Rechtsanwalt Ihres Vertrauens für die massgeschneiderte Ausarbeitung und Prüfung des Vertrags geboten.

Nachtrag zum Datenschutz –

Vertrag zur Auftragsverarbeitung

zwischen

Unternehmen X

als Verantwortlicher (nachfolgend Auftraggeber)

und

Unternehmen Y

als Auftragsverarbeiter (nachfolgend Auftragnehmer)

Präambel

1. Der Auftraggeber und der Auftragnehmer haben am [Datum] eine Vereinbarung [Beschreibung mit Leistungsgegenstand] abgeschlossen (nachfolgend **Hauptvertrag**), in dessen Rahmen der Auftragnehmer für den Auftraggeber Arbeiten oder Dienstleistungen oder gegebenenfalls sonstige Leistungen, wie im Hauptvertrag festgelegt, erbringt.
2. Zum Zwecke der Erfüllung des Hauptvertrags erhält der Auftragnehmer unter Umständen Zu­gang zu personenbezogenen Daten, die dem Auftragnehmer durch den Auftraggeber direkt oder in dessen Auftrag durch Dritte offengelegt oder auf andere Weise zur Verfügung gestellt werden (nachfolgend **personenbezogene Daten**).
3. Die Parteien möchten sicherstellen, dass die durch den Auftragnehmer im Auftrag des Auftragge­bers direkt oder durch Dritte durchgeführte Verarbeitung personenbezogener Daten im Rahmen des Hauptvertrags den geltenden Datenschutzgesetzen entspricht und sich dabei auf bestimmte Bedingungen für die genannte Datenverarbeitung verständigen, die in diesem Nachtrag zum Da­tenschutz (Verantwortlicher – Auftragsverarbeiter) (im Folgenden der **Vertrag**) festgelegt sind.

Dies vorausgeschickt, vereinbaren die Parteien was folgt:

1. **Begriffsdefinitionen**
   1. **Geltende Datenschutzgesetze**meint die Verordnung (EU) 2016|679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (im Folgenden DSGVO), das neu Schweizer Bundesgesetz über den Datenschutz (DSG), die Schweizer Verordnung zum Bundesgesetz über den Datenschutz (DSV) sowie gegebenenfalls sonstige anwendbare Datenschutzerlasse.
   2. **Verantwortlicher** ist die natürliche oder juristische Person, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 4 Abs. 7 DSGVO; Art. 5 lit. j DSG).
   3. **Auftragsverarbeiter** ist die natürliche oder juristische Person, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (Art. 4 Abs. 8 DSGVO; Art. 5 lit. k DSG ).
   4. **Personenbezogene Daten** sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche oder juristische Person (nachfolgend **betroffene Person**) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Austruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann (Art. 4 Abs. 1 DSGVO; Art. 5 lit. a DSG).
   5. **Verarbeitung/Bearbeitung** ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das 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 (Art. 4 Abs. 2 DSGVO;   
      Art. 5 lit. d DSG).
2. **Geltungsbereich und Gegenstand**

2.1. Geltungsbereich

Der vorliegende Vertrag gilt für jede Form der Verarbeitung personenbezogener Daten für den Auftraggeber durch den Auftragnehmer.

2.2. Gegenstand, Dauer, Art und Zweck

Gegenstand und Dauer sowie Art und Zweck der Verarbeitung ergeben sich aus dem Hauptvertrag sowie aus Anlage A, sofern sie nicht bereits im Hauptvertrag und der zugehörigen Leistungsbeschreibung genügend konkretisiert sind.

2.3. Art personenbezogener Daten/Kategorien betroffener Personen

Die Art der personenbezogenen Daten sowie die Kategorien der betroffenen Personen sind in Anlage A spezifiziert, sofern sie nicht bereits im Hauptvertrag und in der zugehörigen Leistungsbeschreibung genügend konkretisiert sind.

1. **Pflichten des Auftragnehmers**
   1. Weisungsgemässe Verarbeitung

Der Auftragnehmer verpflichtet sich, die Daten ausschliesslich für die Zwecke des Hauptvertrags einschliesslich dieses Vertrags sowie gemäss den dokumentierten Instruktionen/Weisungen des Auftraggebers zu verarbeiten. Dies gilt insbesondere auch bezüglich der Übermittlung der Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragnehmer durch das Recht der Europäischen Union, der Mitgliedstaaten oder eines Nicht-EU-Mitgliedstaats, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

Der Auftraggeber kann jederzeit neue Instruktionen erlassen, ergänzen oder bestehende Instruktionen ändern. Dies umfasst auch Instruktionen im Hinblick auf die Berichtigung, Löschung und Sperrung personenbezogener Daten. Alle erteilten Instruktionen sind sowohl vom Auftraggeber als auch vom Auftragnehmer schriftlich oder in elektronisch dokumentierter Form zu dokumentieren.

Ist der Auftragnehmer der Ansicht, dass eine Instruktion des Auftraggebers gegen dateschutzrechtliche Bestimmungen verstösst, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung so lange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Instruktion ablehnen.

Im Übrigen bleiben die Pflichten, die dem Auftragnehmer direkt aus den anwendbaren Datenschutzgesetzen entstehen, wie beispielsweise die Erstellung eines Verzeichnisses der vorliegenden Auftagsverarbeitung gemäss Art. 30 Abs. 2 DSGVO, erhalten und von diesem Vertrag unberührt.

* 1. Pflicht zur Verschwiegenheit

Der Auftragnehmer verpflichtet sich und leistet Gewähr dafür, dass er alle mit der Datenverarbeitung betrauten Personen, einschliesslich Erfüllungsgehilfen, vor Aufnahme der Tätigkeit zur Vertraulichkeit in schriftlicher Form verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen, und dass die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung betrauten Personen auch nach Beendigung ihrer Tätigkeit beim Auftragnehmer bestehen bleibt. Der Auftragnehmer haftet für ein etwaiges Zuwiderhandeln der mit der Datenverarbeitung betrauten Personen, einschliesslich Erfüllungsgehilfen, wie für sein eigenes Verhalten.

* 1. Schutzmassnahmen des Auftragnehmers

Der Auftragnehmer verpflichtet sich und leistet Gewähr dafür, dass er alle erforderlichen Massnahmen zur Gewährleistung der Sicherheit der Verarbeitung gemäss Art. 32 DSGVO bzw. Art. 7 DSG ergriffen hat und aufrechterhält, um eine unbefugte Verarbeitung, einen Verlust oder eine Beschädigung personenbezogener Daten zu verhindern. Dies beinhaltet insbesondere die Mindestvorkehrungen, welche in Anlage B beschrieben sind.

Die TOMs dürfen entsprechend dem technischen Fortschritt weiterentwickelt und durch adäquate Schutzmassnahmen ersetzt werden, sofern sie das Sicherheitsniveau der festgelegten Massnahmen nicht unterschreiten und wesentliche Änderungen dem Auftraggeber mitgeteilt werden.

Die im Rahmen des Vertrages überlassenen personenbezogenen Daten sowie Datenträger und sämtliche hiervon gefertigten Kopien verbleiben im Eigentum des Auftraggebers, sind durch die Auftragnehmerin sorgfältig zu verwahren, vor Zugang durch unberechtigte Dritte zu schützen und dürfen nur mit Zustimmung des Auftraggebers, und dann nur datenschutzgerecht, vernichtet werden. Kopien von personenbezogenen Daten dürfen nur erstellt werden, wenn sie zur Erfüllung der Leistungshaupt- und Nebenpflichten der Auftragnehmerin gegenüber dem Auftraggeber erforderlich sind (z.B. Backups).

* 1. Unterstützungspflichten

Der Auftragnehmer ist verpflichtet, dem Auftraggeber auf Verlangen bei der Einhaltung der geltenden Datenschutzgesetze jederzeit und soweit möglich zu unterstützen.

1. Anträge und Rechte betroffener Personen

Der Auftragnehmer verpflichtet sich, den Auftraggeber mit geeigneten technischen und organisatorischen Massnahmen zu unterstützen, damit der Auftraggeber seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen Personen (insbesondere Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch sowie automatisierte Entscheidungsfindung im Einzelfall) bzw. Art. 8 ff. DSG innerhalb der gesetzlichen Fristen jederzeit nachkommen kann, und überlässt dem Auftraggeber alle dafür notwendigen und ihm zur Verfügung stehenden Informationen.

Wird ein entsprechender Antrag an den Auftragnehmer gerichtet, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten. Der Auftragnehmer muss die Beantwortung solcher Anträge dem Auftraggeber überlassen, es sei denn, er ist gesetzlich dazu verpflichtet. In jedem Fall vereinbaren die Parteien, die Beantwortung solcher Anträge gegenseitig abzusprechen.

1. Weitere Informations- und Unterstützungspflicht

Der Auftragnehmer verpflichtet sich, den Auftraggeber unter Berücksichtigung der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Art. 32 bis 36 DSGVO bzw. Art. 7 DSG genannten Pflichten zu unterstützen (Datensicherheitsmassnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgenabschätzung und vorherige Konsultation).

Der Auftragnehmer verpflichtet sich, den Auftraggeber unverzüglich zu benachrichtigen im Falle

1. eines etwaigen tatsächlichen oder mutmasslichen Datenschutzverstosses (dies gilt auch für Verstösse gegen den Hauptvertrag einschliesslich dieses Vertrags sowie etwaige sonstige Datenschutzverstösse gemäss DSGVO bzw. DSG) unter Angabe sämtlicher dem Auftragnehmer zur Verfügung stehenden Informationen gemäss Artikel 33 Abs. 3 der DSGVO;
2. (ii) etwaiger tatsächlicher oder drohender Beeinträchtigungen oder Mängel aufseiten des Auftragnehmers, die einer Einhaltung der Bestimmungen des Hauptvertrags einschliesslich dieses Vertrags entgegenstehen;
3. (iii) des Vorliegens etwaiger Anträge auf Zugang sowie des tatsächlich erfolgten Zugangs zu personenbezogenen Daten durch Behörden, sofern diese Benachrichtigung nicht per Gesetz aus wichtigen Gründen des öffentlichen Interesses verboten ist.
   1. Rückgabe oder Löschungspflicht bei Vertragsbeendigung

Der Auftragnehmer verpflichtet sich, nach Beendigung des Hauptvertrags einschliesslich dieses Vertrags oder auf Verlangen des Auftraggebers sämtliche personenbezogenen Daten, vorbehaltlich gesetzlicher Aufbewahrungspflichten innerhalb der EU/EWR oder der Schweiz, an den Auftraggeber nach seiner Wahl zurückzugeben oder zu löschen, ohne eine Kopie aufzubewahren, und die Löschung gegenüber dem Auftraggeber entsprechend zu bestätigen.

* 1. Kontrollrechte des Auftraggebers

Der Auftragnehmer verpflichet sich, dem Auftraggeber sämtliche Informationen zur Verfügung zu stellen, die erforderlich sind, um die Einhaltung dieses Vertrags durch den Auftragnehmer nachzuweisen und Überprüfungen, einschliesslich Inspektionen, durch den Auftraggeber selbst, einen vom Auftraggeber beauftragten Prüfer oder durch die Aufsichtsbehörde zu ermöglichen und aktiv zu unterstützen.

Kontrollen beim Auftragnehmer erfolgen innerhalb üblicher Geschäftszeiten, sind von dem Auftraggeber mit einer angemessenen Frist (mindestens 14 Tage, ausser in Notfällen) anzumelden und durch den Auftragnehmer zu unterstützen (z.B. durch Bereitstellung von Personal).

Die Kontrollen sind auf den erforderlichen Rahmen beschränkt und müssen auf Betriebs- und Geschäftsgeheimnisse des Auftragnehmers sowie den Schutz von Personendaten Dritter (z.B. anderer Kunden oder Mitarbeiter des Auftragnehmers) Rücksicht nehmen.

[Anmerkung: je nachdem, ob vorliegend der Auftraggeber oder der Auftragnehmer Vertragsinhaber ist, kann das Kontrollrecht unterschiedlich mehr im Interesse des Auftraggebers bzw. mehr im Interesse des Auftragnehmers ausgestaltet sein]

1. **Ort der Durchführung der Datenverarbeitung**

Die Datenverarbeitungen werden nur an den Standorten durchgeführt, die im zugehörigen Hauptvertrag oder in diesem Vertrag in Anlage C vereinbart oder anderweitig vom Auftraggeber schriftlich oder in elektronisch dokumentierter Form genehmigt wurden.

Der Auftragnehmer verpflichtet sich, keine personenbezogenen Daten, auch nicht teilweise, ohne vorgängige schriftliche oder elektronisch dokumentierte Zustimmung des Auftraggebers an ein Drittland zu übermitteln.

Werden die Datenverarbeitungstätigkeiten, wenn auch nur teilweise, auch ausserhalb der EU durchgeführt, muss vorgängig ein agemessenes Datenschutzniveau mittels der nachfolgend aufgeführten geeigneten Garantien sichergestellt werden (vgl. Art. 45 ff. DSGVO bzw. Art. 16 DSG)[[4]](#footnote-4):

* Angemessenheitsbeschluss der Europäischen Kommission sowie des Eidgenössischen Datenschutzbeauftragten (EDÖB) bzw. des Bundesrates;
* Standarddatenschutzklauseln der EU-Kommission;
* verbindliche interne Datenschutzvorschriften (sog. binding corporate rules);
* von einer Aufsichtbehörde bewilligte Standarddatenschutzklauseln;
* von der zuständigen Aufsichtsbehörte genehmigte Verhaltensregeln (sog. Code of Conduct);
* durch einen genehmigten Zertifizierungsmechanismus;
* eine von der DSGVO bzw. vom nDSG vorgesehenen Ausnahme für bestimmte Fälle sowie für Einzelfälle.

Die angewendeten geeigneten Garantien für eine Datenübermittlung sind in Anlage D konkretisiert und soweit notwendig dokumentiert.

1. **Einsatz von Unterauftragsverarbeitern**

Der Auftragnehmer ist nicht berechtigt, einen Unterauftragsverarbeiter heranzuziehen, ohne vor-gängig die schriftliche oder elektronisch dokumentierte Zustimmung des Auftraggebers einzuholen.

Der Auftragnehmer ist befugt, die im Anhang E aufgeführten Unternehmen als Unterauftrags-verarbeiter heranzuziehen.

Beabsichtigte Änderungen des Unterauftragsverarbeiters sind dem Auftraggeber rechtzeitig schriftlich bekannt zu geben, sodass er diese gegebenenfalls untersagen kann. Der Auftragnehmer schliesst die erforderlichen schriftlichen Vereinbarungen zur Vertraulichkeit und zum Datenschutz mit dem Unterauftragsverarbeiter ab, welche mindestens so streng wie die Bestimmungen des Hauptvertrags einschliesslich dieses Vertrags sein müssen. Dabei hat der Auftragnehmer insbesondere sicherzustellen, dass der Unterauftragsverarbeiter dieselben Verpflichtungen eingeht und insbesondere auch die technischen und organisatorischen Massnahmen trifft, die dem Auftragnehmer aufgrund dieses Vertrags obliegen.

Der Auftragnehmer haftet gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Unterauftragsverarbeiters wie für sein eigenes Verhalten.

1. **Ausführung zusätzlicher Vereinbarungen**

Der Auftragnehmer stimmt zu, auf Verlangen des Auftraggebers im Rahmen der bestehenden Verträge weiterführende Vereinbarungen mit dem Auftraggeber zur Verarbeitung personenbezogener Daten abzuschliessen, sofern der Auftraggeber dies nach vernünftigem Ermessen für die Einhaltung des geltenden Datenschutzrechts als erforderlich erachtet.

1. **Ausserordentliches Kündigungsrecht**

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoss des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrags vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Dabei stellen insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO bzw. Art. 9 DSG abgeleiteten Pflichten einen schweren Verstoss dar.

1. **Bezug zu bestehenden Verträgen**
   1. Die Anlagen zu diesem Vertrag bilden einen integrierenden Bestandteil des vorliegenden Vertrags.
   2. Steht eine in diesem Vertrag enthaltene Bestimmung im Widerspruch zum Hauptvertrag, gilt die im vorliegenden Vertrag enthaltene Bestimmung als massgeblich.
   3. Die Bestimmungen des vorliegenden Vertrags haben auch nach Beendigung des Hauptvertrags weiterhin Bestand, solange der Auftragnehmer im Besitz personenbezogener Daten des Auftraggebers ist.
2. **Schlussbestimmungen**
   1. Änderungen und Ergänzungen dieses Vertrags bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
   2. Sollten einzelne Bestimmungen dieses Vertrags ganz oder teilweise ungültig sein oder werden, so wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. Die Parteien vereinbaren, die unwirksame Bestimmung durch eine wirksame Bestimmung zu ersetzen, welche dem wirtschaftlichen Sinn und Zweck der unwirksamen Bestimmung am nächsten kommt.
   3. Dieser Vertrag untersteht Schweizer Recht unter Ausschluss des Internationalen Privatrechts (IPRG). Ausschliesslicher Gerichtsstand für Streitigkeiten aus diesem Vertrag oder im Zusammenhang mit der Auslegung und Anwendung des vorliegenden Vertrags ist der Sitz des Auftraggebers.

**ANLAGEN**

Anlage A: Auftragspezifizierung

Anlage B: Technische und organisatorische Massnahmen – Mindestvorkehrungen

Anlage C: Genehmigte Datenverarbeitungsstandorte

Anlage D: Geeignete Garantien für die Datenübermittlung

Anlage E: Zugelassene Unterauftragsverarbeiter

|  |  |
| --- | --- |
| **[**Ort, Datum**]**  **[Auftraggeber]** |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **[Name]**  **[**Position**]** | **[Name]**  **[**Position**]** |
| **[**Ort, Datum**]**  **[Auftragnehmer]** |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **[Name]**  **[**Position**]** | **[Name]**  **[**Position**]** |

**Anlage A: Auftragsspezifizierung**

1. **Auftragsspezifizierung**
   1. **Gegenstand, Art und Zweck der Verarbeitung**

Gegenstand, Art und Zweck dieses Auftrags ist die Durchführung folgender Aufgaben:

*[Möglichst detaillierte Beschreibung der Aufgaben des Auftragnehmers, einschliesslich Art und Zweck der vorgesehenen Verarbeitung].*

* 1. **Dauer der Verarbeitung**

Die Verarbeitung gilt für folgende Dauer:

*[Konkrete Dauer der Verarbeitung festlegen*].

* 1. **Art der personenbezogenen Daten**

Zur Erfüllung der Aufgaben werden folgende Datenkategorien verarbeitet:

*[Datenkategorien aufzählen, z.B. Kontaktdaten, Vertragsdaten, Verrechnungsdaten, Bonitätsdaten, Bestelldaten, Entgeltdaten usw]*.

* 1. **Kategorien der betroffenen Personen**

Die Datenverarbeitung bezieht sich auf folgende Kategorien betroffener Personen:

*[Betroffenenkategorien ergänzen, z.B. Kunden, Interessenten, Lieferanten, Ansprechpartner, Beschäftigte usw.].*

**Anlage B: Technische und organisatorische Massnahmen – Mindestvorkehrungen**

Im Folgenden werden die auf Art. 32 DSGVO bzw. Art. 7 DSG und Art. 8 ff. VDSG[[5]](#footnote-5) basierenden technischen und organisatorischen Massnahmen beschrieben, die konkret vom Auftragnehmer im Zusammenhang mit der Verarbeitung personenbezogener Daten und der Erfüllung seiner Verpflichtungen gemäss dem Hauptvertrag einschliesslich diesem Vertrag als Mindestvorkehrungen zu ergreifen sind, um ein dem Risiko angemessenes Schutzniveau hinsichtlich des Datenschutzes und der Datensicherheit der überlassenen Daten zu gewährleisten.

[Anmerkung: vgl. dazu auch den Leitfaden des EDÖB zu den technischen und organisatorischen Massnahmen unter <https://www.edoeb.admin.ch/edoeb/de/home/kurzmeldungen/km2024/23012024_leitfaden_tom.html>].

1. **Gewährleistung der Vertraulichkeit**
2. **Zugriffskontrolle**

Der Auftragnehmer gewährleistet, dass ausschliesslich berechtigte Personen nur auf diejenigen Personendaten Zugriff haben, die sie zur Erfüllung ihrer Aufgaben benötigen.

Mögliche Massnahmen: z.B. Standard-Berechtigungsprofile auf «Need-to-know-Basis», Standardprozess für Berechtigungsvergabe, Protokollierung von Zugriffen, periodische Überprüfung der vergebenen Berechtigungen, insbesondere von administrativen Benutzerkonten.

Der Auftragnehmer gewährleistet die Zugriffskontrolle durch folgende Massnahmen:

*Beschreibung der konkreten Massnahmen:*

1. **Zugangskontrolle**

Der Auftragnehmer gewährleistet, dass nur berechtigte Personen Zugang zu den Räumlichkeiten und Anlagen haben, in denen Personendaten bearbeitet werden.

*Mögliche Massnahmen: z.B. Schlüssel, Magnet- oder Chipkarten, elektrische Türöffner, Portier, biometrischer Ausweis, Sicherheitspersonal, Alarmanlagen, Videoanlagen.*

Der Auftragnehmer gewährleistet die Zugangskontrolle durch folgende Massnahmen:

*Beschreibung der konkreten Massnahmen:*

1. **Benutzerkontrolle**

Der Auftragnehmer gewährleistet, dass unbefugte Personen automatisierte Datenbearbeitungssysteme nicht mittels Einrichtungen zur Datenübertragung benutzen können.

*Mögliche Massnahmen: z.B. Kennwörter, Passwörter (einschliesslich entsprechender Policy), automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern, Virenschutz.*

Der Auftragnehmer gewährleistet die Benutzerkontrolle durch folgende Massnahmen:

*Beschreibung der konkreten Massnahmen:*

1. **Gewährleistung der Verfügbarkeit und Integrität**
2. **Datenträgerkontrolle**

Der Auftragnehmer gewährleistet, dass unbefugte Personen Datenträger nicht lesen, kopieren, verändern, verschieben, löschen oder vernichten können.

*Mögliche Massnahmen: z.B. Back-up-Strategie zwecks Datensicherung und Wiederherstellung (online/offline; on-site/off-site), physische Löschung von Datenträgern, unterbrechungsfreie Stromversorgung (USV, Dieselaggregat), Virenschutz, Firewall, Meldewege und Notfallpläne; Security-Checks auf Infrastruktur- und Applikationsebene, mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum, Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern, Löschungsfristen sowohl für Daten selbst als auch Metadaten wie Logfiles u.Ä.*

Der Auftragnehmer gewährleistet die Datenträgerkontrolle durch folgende Massnahmen:

*Beschreibung der konkreten Massnahmen:*

1. **Speicherkontrolle**

Der Auftragnehmer gewährleistet, dass unbefugte Personen Personendaten im Speicher nicht speichern, lesen, ändern, löschen oder vernichten können.

*Mögliche Massnahmen: z.B. Protokollierung, wer, wann, welche Daten eingeben oder ändern darf, Stellvertreterregelungen, Protokollierung von Datenänderungen, Dokumentenmanagement, keine Zwischenspeicherung, etc.*

Der Auftragnehmer gewährleistet die Speicherkontrolle durch folgende Massnahmen:

*Beschreibung der konkreten Massnahmen:*

1. **Transportkontrolle**

Der Auftragnehmer gewährleistet, dass unbefugte Personen bei der Bekanntgabe von Personendaten oder beim Transport von Datenträgern Personendaten nicht lesen, kopieren, verändern, löschen oder vernichten können.

*Mögliche Massnahmen: z.B. Berechtigungskonzept, Verschlüsselung, Virtual Private Networks (VPN), Protokollierung der Übermittlung und der Empfänger, elektronische Signatur.*

Der Auftragnehmer gewährleistet die Transportkontrolle durch folgende Massnahmen:

*Beschreibung der konkreten Massnahmen:*

1. **Wiederherstellung**

Der Auftragnehmer gewährleistet, dass die Personendaten und der Zugang zu ihnen bei einem psychischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

*Mögliche Massnahmen: z.B. Generelles Datensicherheitskonzept, Kontrollierte und regelmässige Sicherung der Benutzerdateien, Datenbanken, Kennzeichnung der Datenträger, Verwendung des Schreibschutzes bei Datenträgern, Archivordnung, Protokollierungen, Back-up-Strategie zwecks Datensicherung und Wiederherstellung (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV, Dieselaggregat), Virenschutz, Firewall, Meldewege und Notfallpläne; Security-Checks auf Infrastruktur- und Applikationsebene, mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum, Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern, Löschungsfristen sowohl für Daten selbst als auch Metadaten wie Logfiles u.Ä.*

etc.

Der Auftragnehmer gewährleistet die Wiederherstellung durch folgende Massnahmen:

*Beschreibung der konkreten Massnahmen:*

1. **Datenintegrität**

Der Auftragnehmer gewährleistet, dass alle Funktionen des automatisierten Datenbearbeitungssystems zur Verfügung stehen (Verfügbarkeit), Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte Personendaten nicht durch Fehlfunktionen des Systems beschädigt werden können.

*Mögliche Massnahmen: z.B. Unterbrechungsfreie Stromversorgung (UPS), Vorrichtungen, um Temperatur und Feuchtigkeit in Serverräumen zu überwachen, Feuer- und Rauchmeldesysteme, Alarmierung bei unbefugten Zutritten, Schaffung von Backup- und Wiederherstellungskonzepten, Protokollierung, Erstellen von Datenbackups, Testen der Datenwiederherstellung, Notfallpläne, Prüfung der Notfalleinrichtungen, etc.*

Der Auftragnehmer gewährleistet die Datenintegrität durch folgende Massnahmen:

Beschreibung *der konkreten Massnahmen:*

1. **Systemsicherheit**

Der Auftragnehmer gewährleistet, dass Betriebssysteme und Anwendungssoftware stets auf dem neusten Sicherheitsstand gehalten und bekannte kritische Lücken geschlossen werden.

*Mögliche Massnahmen: z.B. Regelmässige Überprüfung und Testen, Weiterbildung technisches Wissen der IT- und IT-Sicherheitsfunktionen, Datenschutzmanagement, einschliesslich regelmässiger Mitarbeiterschulungen; Incident-Response-Management; datenschutzfreundliche Voreinstellungen (Privacy by Design & Privacy by Default), unverzügliche Behebung von entdeckten Mängeln*.

Der Auftragnehmer gewährleistet die Systemsicherheit durch folgende Massnahmen:

*Beschreibung der konkreten Massnahmen:*

1. **Gewährleistung der Nachvollziehbarkeit**
2. **Eingabekontrolle**

Der Auftragnehmer gewährleistet die Eingabekontrolle, damit überprüft werden kann, welche Personendaten zu welcher Zeit und von welcher Person im automatisierten Datenbearbeitungssystem eingegeben oder verändert werden.

*Mögliche Massnahmen: z.B. Berechtigungskonzept, Zuständigkeiten für die Dateneingabe (einschliesslich Regelung der Stellvertretung), Automatische Dokumentation der Eingabeberechtigungen, Protokollierung etc.*

Der Auftragnehmer gewährleistet die Eingabekontrolle durch folgende Massnahmen:

*Beschreibung der konkreten Massnahmen:*

1. **Bekanntgabekontrolle**

Der Auftragnehmer gewährleistet die Bekanntgabekontrolle, damit überprüft werden kann, wem Personendaten mit Hilfe von Einrichtungen zur Datenübertragung bekannt gegeben werden.

*Mögliche Massnahmen: z.B. Schaffung einer Standleitung oder einer VPN-Verbindung, Verschlüsselung, TLS Verschlüsselung für alle Kommunikation, Pseudonymisierung, Implementierung von Sicherheitsgateways an den Netzübergabepunkten, Datenschutzgerechtes Lösch-/Zerstörungsverfahren, .*

Der Auftragnehmer gewährleistet die Bekanntgabekontrolle durch folgende Massnahmen:

*Beschreibung der konkreten Massnahmen:*

1. **Erkennung und Beseitigung**

Der Auftragnehmer gewährleistet die Erkennung und Beseitigung, damit Verletzungen der Datensicherheit rasch erkannt und Massnahmen zur Minderung oder Beseitigung der Folgen ergriffen werden können.

*Mögliche Massnahmen: z.B. Sicherheits- und Fehlermeldungskonzepte, Testverfahren etc.*

Der Auftragnehmer gewährleistet die Erkennung und Beseitigung durch folgende Massnahmen:

*Beschreibung der konkreten Massnahmen:*

1. **Weitere Massnahmen**
2. **Trennungskontrolle: Anforderung: es muss gewährleistet sein, dass Daten, die für verschiedene Zwecke erhoben wurden, getrennt verarbeitet werden können**

Der Auftragnehmer gewährleistet die getrennte Verarbeitung von Daten durch geeignete Massnahmen. Insbesondere müssen zu unterschiedlichen Zwecken erhobene Personendaten getrennt verarbeitet werden.

*Mögliche Massnahmen: z.B. Trennung von Produktiv- und Testumgebung, physikalische Trennung (Systeme/Datenbanken / Datenträger), Festlegung von Datenbankrechten, etc.*

Der Auftragnehmer gewährleistet die Trennungskontrolle durch folgende Massnahmen:

*Beschreibung der konkreten Massnahmen:*

1. **Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung**

Der Auftragnehmer gewährleistet die Implementierung eines Verfahrens zur regelmässigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Massnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

*Mögliche Massnahmen: Datenschutzmanagement, einschliesslich regelmässiger Mitarbeiterschulungen; Incident-Response-Management; datenschutzfreundliche Voreinstellungen (Privacy by Design & Privacy by Default), unverzügliche Behebung von entdeckten Mängeln.*

Der Auftragnehmer gewährleistet die Erkennung und Beseitigung durch folgende Massnahmen:

*Beschreibung der konkreten Massnahmen:*

1. **Auftragskontrolle: Auftragsdatenverarbeitung im Sinne von Art. 9 DSG nur auf Anweisung des Auftraggebers**

Der Auftragnehmer gewährleistet, dass die Unterauftragsbearbeiter die Personendaten nur auf Anweisung des Auftraggebers und unter Gewährleistung der Datensicherheit mittels eines schriftlichen Auftragsbearbeitungsvertrages bearbeiten.

*Mögliche Massnahmen: z.B. formalisiertes Auftragsmanagement, strenge Auswahl des Unterauftragsverarbeiters (ISO-Zertifizierung, ISMS), eindeutige schriftliche Vertragsgestaltung mit dem Unterauftragsverarbeiter, Überprüfung der Einhaltung dieser Verträge durch die Unterauftragsverarbeiter, Vorabüberzeugungspflicht, Nachkontrollen.*

Der Auftragnehmer gewährleistet die Erkennung und Beseitigung durch folgende Massnahmen:

*Beschreibung der konkreten Massnahmen:*

1. **Pseudonymisierung**

Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der Personendaten in der jeweiligen Datenanwendung entfernt und gesondert aufbewahrt.

*Beschreibung der konkreten Massnahmen:*

**Allfällige weitere Massnahmen**

**Anlage C: Genehmigte Datenverarbeitungsstandorte**

*[Firma, Standort und Land der Datenverarbeitung ergänzen]*

**Anlage D: Geeignete Garantien für die Datenübermittlung**

*[Beschreibung und Dokumentation]*

**Anlage E: Zugelassene Unterauftragsverarbeiter**

*[Firmenname, Sitz, Land und Art der Tätigkeiten ergänzen]*

ANHANG I

Relevante Gesetzesbestimmungen

in der DSGVO

**Kapitel IV – Verantwortlicher und Auftragsbearbeiter**

**Abschnitt 1 – Allgemeine Pflichten**

**Art. 28 – Auftragsverarbeiter**

1. Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.
2. Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.
3. Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind. Dieser Vertrag bzw. dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter
   1. die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, 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;
   2. gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
   3. alle gemäß [Artikel 32](https://dsgvo-gesetz.de/art-32-dsgvo/) erforderlichen Maßnahmen ergreift;
   4. die in den Absätzen 2 und 4 genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;
   5. angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in [Kapitel III](https://dsgvo-gesetz.de/kapitel-3/) genannten Rechte der betroffenen Person nachzukommen;
   6. unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den [Artikeln 32](https://dsgvo-gesetz.de/art-32-dsgvo/) bis [36](https://dsgvo-gesetz.de/art-36-dsgvo/) genannten Pflichten unterstützt;
   7. nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt und die vorhandenen Kopien löscht, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht;
   8. dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt.

Mit Blick auf Unterabsatz 1 Buchstabe h informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen diese Verordnung oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

1. Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in dem Vertrag oder anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter gemäß Absatz 3 festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden muss, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen dieser Verordnung erfolgt. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.
2. Die Einhaltung genehmigter Verhaltensregeln gemäß [Artikel 40](https://dsgvo-gesetz.de/art-40-dsgvo/) oder eines genehmigten Zertifizierungsverfahrens gemäß [Artikel 42](https://dsgvo-gesetz.de/art-42-dsgvo/) durch einen Auftragsverarbeiter kann als Faktor herangezogen werden, um hinreichende Garantien im Sinne der Absätze 1 und 4 des vorliegenden Artikels nachzuweisen.
3. Unbeschadet eines individuellen Vertrags zwischen dem Verantwortlichen und dem Auftragsverarbeiter kann der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 des vorliegenden Artikels ganz oder teilweise auf den in den Absätzen 7 und 8 des vorliegenden Artikels genannten Standardvertragsklauseln beruhen, auch wenn diese Bestandteil einer dem Verantwortlichen oder dem Auftragsverarbeiter gemäß den [Artikeln 42](https://dsgvo-gesetz.de/art-42-dsgvo/) und [43](https://dsgvo-gesetz.de/art-43-dsgvo/) erteilten Zertifizierung sind.
4. Die Kommission kann im Einklang mit dem Prüfverfahren gemäß [Artikel 93](https://dsgvo-gesetz.de/art-93-dsgvo/) Absatz 2 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.
5. Eine Aufsichtsbehörde kann im Einklang mit dem Kohärenzverfahren gemäß [Artikel 63](https://dsgvo-gesetz.de/art-63-dsgvo/) Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.
6. Der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.
7. Unbeschadet der [Artikel 82](https://dsgvo-gesetz.de/art-82-dsgvo/), [83](https://dsgvo-gesetz.de/art-83-dsgvo/) und [84](https://dsgvo-gesetz.de/art-84-dsgvo/) gilt ein Auftragsverarbeiter, der unter Verstoß gegen diese Verordnung die Zwecke und Mittel der Verarbeitung bestimmt, in Bezug auf diese Verarbeitung als Verantwortlicher.

1. Bundesgesetz vom 25. September 2020 über den Datenschutz (DSG), rechtskräftig per 1. September 2023. [↑](#footnote-ref-1)
2. Die Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (DS-GVO) kann unter der Website <http://eur-lex.europa.eu/eli/reg/2016/679/oj> abgerufen werden. [↑](#footnote-ref-2)
3. Die Standarddatenschutzklauseln der EU-Kommission (EU-Model-Contracts) können unter der folgenden Seite abgerufen werden: <https://ec.europa.eu/info/law/law-topic/data-protection_de>. [↑](#footnote-ref-3)
4. Nichtzutreffendes soll bitte gelöscht werden. [↑](#footnote-ref-4)
5. Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG). [↑](#footnote-ref-5)