

Anlage zur Auftragsverarbeitung gemäß Art. 28 DS-GVO zu Vertragsnummer: 10048442

Auftragnehmer (Name, Adresse, Land):

Inhalt

- Klauseln 1 bis 11
- [Anhang I – Beschreibung der Verarbeitung](#)
- [Anhang II – Liste der Unterauftragnehmer](#)
- [Anhang III – Technische und organisatorische Maßnahmen \(TOM\)](#)

Klausel 1 - Zweck und Anwendungsbereich

- a) Mit dieser Anlage zur Auftragsverarbeitung (im Folgenden „Klauseln“) soll die Einhaltung von Artikel 28 Absätze 3 und 4 der 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 (**Datenschutz-Grundverordnung**) sichergestellt werden.
- b) Die Auftraggeberin als Verantwortliche und der Auftragnehmer als Auftragsverarbeiter (im Folgenden „die Parteien“) haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 zu gewährleisten.
- c) Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anhang I.
- d) Die Anhänge I bis III sind Bestandteil der Klauseln.
- e) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen die Auftraggeberin gemäß der Verordnung (EU) 2016/679 unterliegt.
- f) Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 erfüllt werden. Findet eine Übermittlung personenbezogener Daten durch die Auftraggeberin an den Auftragnehmer in ein Drittland statt, ist für diese Datenübermittlung eine Rechtsgrundlage erforderlich. Falls weder ein Angemessenheitsbeschluss nach Artikel 45 der Verordnung (EU) 2016/679 vorliegt noch geeignete Garantien nach Artikel 46 der Verordnung (EU) 2016/679 bestehen und auch keine der Ausnahme für einen bestimmten Fall gemäß Art. 49 der Verordnung (EU) 2016/679 anwendbar ist, wird zur Schaffung einer Rechtsgrundlage eine rechtsverbindliche Vereinbarung zwischen Auftraggeberin und Auftragnehmer geschlossen. Diese besteht im Abschluss von Standarddatenschutzklauseln gemäß Artikel 46 Absatz 1 und Artikel 46 Absatz 2 Buchstabe c der Verordnung (EU) 2016/679.

Klausel 2 - Unabänderbarkeit der Klauseln

Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen. Ergänzungen oder Aktualisierungen der in den Anhängen angegebenen Informationen bedürfen keiner schriftlichen Vertragsergänzung und können in Textform vereinbart werden.

Klausel 3 - Auslegung

- a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.
- b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 auszulegen.
- c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Klausel 4 - Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

Klausel 5 - Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag der Auftraggeberin verarbeitet werden, sind in Anhang I aufgeführt.

Klausel 6 - Pflichten der Parteien**6.1 Weisungen**

- a) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf dokumentierte Weisung der Auftraggeberin, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragnehmer der Auftraggeberin diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Die Auftraggeberin kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Eine Weisung ist die auf einen bestimmten Umgang des Auftragnehmers mit Daten gerichtete schriftliche, elektronische oder mündliche Anordnung der Auftraggeberin. Die Anordnungen sind zu dokumentieren. Die Weisungen werden zunächst durch die Leistungsbeschreibung definiert und können von der Auftraggeberin danach in dokumentierter Form durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden.
- b) Der Auftragnehmer informiert die Auftraggeberin unverzüglich, wenn er der Auffassung ist, dass von der Auftraggeberin erteilte Weisungen gegen die Verordnung (EU) 2016/679 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.
- c) Die Auftraggeberin kann jederzeit die Herausgabe, Berichtigung, Anpassung, Löschung und Einschränkung der Verarbeitung der Daten verlangen.

- d) Auskünfte an Dritte oder die betroffene Person darf der Auftragnehmer nur nach vorheriger ausdrücklicher Zustimmung durch die Auftraggeberin erteilen. Die Zustimmung ist durch den Auftragnehmer zu dokumentieren.

6.2 Zweckbindung

Der Auftragnehmer verarbeitet die personenbezogenen Daten nur für die in Anhang I genannten spezifischen Zwecke, sofern er keine weiteren Weisungen der Auftraggeberin erhält.

6.3 Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragnehmer nur für die in Anhang I angegebene Dauer verarbeitet.

6.4 Sicherheit der Verarbeitung

- a) Der Auftragnehmer ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.
- b) Dem Auftragnehmer ist es aufgrund des technischen Fortschritts gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der in dem Anhang III festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.
- c) Der Auftragnehmer gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

6.5 Sensible Daten

Falls die Verarbeitung personenbezogener Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten“), wendet der Auftragnehmer angemessene und spezifische Maßnahmen an, die an die spezifische Art der Daten und die damit verbundenen Risiken angepasst sind. Dies kann bspw. die Beschränkung des Personals, das Zugriff auf die personenbezogenen Daten hat, oder auch die Sicherstellung der Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste umfassen.

6.6 Dokumentation und Einhaltung der Klauseln

- a) Der Auftragnehmer bearbeitet Anfragen der Auftraggeberin bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.
- b) Der Auftragnehmer stellt der Auftraggeberin auf deren Wunsch Informationen zur Verfügung, die die Auftraggeberin zur vollständigen Führung des Verzeichnis von Verarbeitungstätigkeiten i.S.d. Artikel 30 Abs. 1 der Verordnung (EU) 2016/679 benötigt.
- c) Der Auftragnehmer informiert die Auftraggeberin unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden oder falls eine Aufsichtsbehörde im Rahmen ihrer Zuständigkeit bei dem Auftragnehmer anfragt, ermittelt oder sonstige Erkundigungen einzieht.
- d) Der Auftragnehmer stellt der Auftraggeberin alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 hervorgehenden Pflichten erforderlich sind. Auf Verlangen der Auftraggeberin gestattet der Auftragnehmer ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann die Auftraggeberin einschlägige Zertifizierungen des Auftragnehmers berücksichtigen.
- e) Die Auftraggeberin kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragnehmers umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.
- f) Die Parteien stellen der zuständigen Aufsichtsbehörde die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

Klausel 7 - Einsatz von Unterauftragnehmern

- a) Der Auftragnehmer darf keinen seiner Verarbeitungsvorgänge, die er im Auftrag der Auftraggeberin gemäß diesen Klauseln durchführt, ohne vorherige gesonderte dokumentierte Zustimmung der Auftraggeberin an einen Unterauftragnehmer (weitere Auftragsverarbeiter) untervergeben. Der Auftragnehmer reicht den Antrag auf die gesonderte Zustimmung mindestens 20 Kalendertage vor der beabsichtigten Beauftragung des betreffenden Unterauftragnehmers zusammen mit den Informationen ein, die die Auftraggeberin benötigt, um über die Zustimmung zu entscheiden. Die Informationen umfassen mindestens den vollständigen Namen inkl. Anschrift und Land des Unterauftragnehmers sowie eine Beschreibung der Verarbeitung durch den Unterauftragnehmer (inkl. Gegenstand, Art und Dauer). Die Auftraggeberin stimmt der Beauftragung der in Anhang II benannten Unterauftragnehmer zu. Die Parteien halten Anhang II jeweils auf dem neuesten Stand.
- b) Sollte der Einsatz von Unterauftragnehmern (weitere Auftragsverarbeiter) ausgeschlossen sein, so ist dies durch die Auftraggeberin in Anhang II festgelegt.

- c) Beauftragt der Auftragnehmer einen Unterauftragnehmer mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag der Auftraggeberin), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragnehmer mindestens dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragnehmer gemäß diesen Klauseln gelten. Der Auftragnehmer stellt sicher, dass der Unterauftragnehmer die Pflichten erfüllt, denen der Auftragnehmer entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 unterliegt.
- d) Der Auftragnehmer stellt der Auftraggeberin auf deren Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragnehmer den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.
- e) Der Auftragnehmer haftet gegenüber der Auftraggeberin in vollem Umfang dafür, dass der Unterauftragnehmer seinen Pflichten gemäß dem mit dem Auftragnehmer geschlossenen Vertrag nachkommt. Der Auftragnehmer benachrichtigt die Auftraggeberin, wenn der Unterauftragnehmer seine vertraglichen Pflichten nicht erfüllt. Der Auftragnehmer hat in diesem Falle auf Verlangen der Auftraggeberin die Beschäftigung des Unterauftragnehmers ganz oder teilweise zu beenden oder das Vertragsverhältnis mit dem Unterauftragnehmer zu lösen, wenn und soweit dies nicht unverhältnismäßig ist.
- f) Nicht als Leistungen von Unterauftragnehmern im Sinne dieser Klauseln gelten Dienstleistungen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung der Auftragsdurchführung in Anspruch nimmt, beispielsweise Telekommunikationsdienstleistungen. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten der Auftraggeberin auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.
- g) Der Auftragnehmer vereinbart mit dem Unterauftragnehmer eine Drittbegünstigtenklausel, wonach die Auftraggeberin – im Falle, dass der Auftragnehmer faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragnehmer anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

Klausel 8 - Internationale Datenübermittlungen

- a) 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.
- b) Jede Übermittlung von Daten durch den Auftragnehmer an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen der Auftraggeberin oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragnehmer unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 im Einklang stehen.

- c) Die Auftraggeberin erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragnehmer einen Unterauftragnehmer gemäß Klausel 7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag der Auftraggeberin) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragnehmer und der Unterauftragnehmer die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

Klausel 9 - Unterstützung der Auftraggeberin

- a) Der Auftragnehmer unterrichtet die Auftraggeberin unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde von der Auftraggeberin dazu ermächtigt.
- b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragnehmer die Auftraggeberin bei der Erfüllung von ihrer Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragnehmer die Weisungen der Auftraggeberin.
- c) Abgesehen von der Pflicht des Auftragnehmers, die Auftraggeberin gemäß Klausel 9 Buchstabe b zu unterstützen, unterstützt der Auftragnehmer unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen die Auftraggeberin zudem bei der Einhaltung der folgenden Pflichten:
1. Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;
 2. Pflicht zur Konsultation der zuständigen Aufsichtsbehörde vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern die Auftraggeberin keine Maßnahmen zur Eindämmung des Risikos trifft;
 3. Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragnehmer die Auftraggeberin unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;
 4. Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679.
- d) Die Parteien legen in Anhang III die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung der Auftraggeberin durch den Auftragnehmer bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

Klausel 10 - Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragnehmer mit der Auftraggeberin zusammen und unterstützt sie entsprechend, damit die Auftraggeberin ihren Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 nachkommen kann, wobei der Auftragnehmer die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

10.1 Verletzung des Schutzes der von der Auftraggeberin verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den von der Auftraggeberin verarbeiteten Daten unterstützt der Auftragnehmer die Auftraggeberin wie folgt:

- a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige Aufsichtsbehörde, nachdem der Auftraggeberin die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);
- b) bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 in der Meldung der Auftraggeberin anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:
 - 1) die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
 - 2) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
 - 3) die von der Auftraggeberin ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

- c) bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679, die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

10.2 Verletzung des Schutzes der vom Auftragnehmer verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragnehmer verarbeiteten Daten meldet der Auftragnehmer diese der Auftraggeberin unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

- a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);
- b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;
- c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragnehmer zur Verfügung zu stellen hat, um die Auftraggeberin bei der Erfüllung von ihren Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679 zu unterstützen.

Klausel 11 - Verstöße gegen die Klauseln und Beendigung des Vertrags

- a) Falls der Auftragnehmer seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann die Auftraggeberin – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 – den Auftragnehmer anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragnehmer unterrichtet die Auftraggeberin unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.
- b) Die Auftraggeberin ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn
 - 1) die Auftraggeberin die Verarbeitung personenbezogener Daten durch den Auftragnehmer gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;
 - 2) der Auftragnehmer in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 nicht erfüllt;

- 3) der Auftragnehmer einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde, die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 zum Gegenstand hat, nicht nachkommt.

Kündigt die Auftraggeberin aus einem der zuvor genannten Gründe, so ist die Kündigung vom Auftragnehmer nach Ziffer 5.3.2 der AVB zu vertreten.

- c) Der Auftragnehmer ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn die Auftraggeberin auf der Erfüllung ihrer Anweisungen besteht, nachdem sie vom Auftragnehmer darüber in Kenntnis gesetzt wurde, dass ihre Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 6.1 Buchstabe b) verstoßen.
- d) Nach Beendigung des Vertrags gibt der Auftragnehmer alle im Auftrag der Auftraggeberin verarbeiteten personenbezogenen Daten an die Auftraggeberin zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragnehmer weiterhin die Einhaltung dieser Klauseln.
- e) Überlassene Datenträger und Datensätze verbleiben im Eigentum der Auftraggeberin.

Anhang I – Beschreibung der Verarbeitung

Die nachfolgende Auswahl wurde durch die Auftraggeberin getroffen. Sollten dem Auftragnehmer im Rahmen des Vergabeverfahrens oder der Auftragsausführung Lücken, Fehler oder Unklarheiten auffallen, so hat ein Hinweis an die Auftraggeberin zu erfolgen.

Art, Zweck und Dauer der Verarbeitung

- ☒ Gegenstand und Dauer der Auftragsverarbeitung sowie Umfang, Art und Zweck der Verarbeitung von personenbezogenen Daten bestimmen sich nach der Leistungsbeschreibung sowie nach dem vom Auftragnehmer eingereichten Angebot.
- ☐ Nähere Beschreibung von Umfang, Art und Zweck der Verarbeitung:

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden

- ☒ Mitarbeiter*Innen der Auftraggeberin einschließlich Bewerber*Innen
- ☐ Abonnent*Innen z.B. von Zeitschriften und Newslettern
- ☐ Externe Veranstaltungsteilnehmende
- ☐ Teilnehmende an Umfragen
- ☐ Besucher*Innen von Räumlichkeiten der Auftraggeberin
- ☐ Besucher*Innen von Webseiten
- ☐ Dienstleister*Innen / Lieferant*Innen
- ☐ Ansprechpartner*Innen von Partnerinstitutionen
- ☐ Vertreter*Innen von öffentlichen Stellen und Regierungsvertreter*Innen
- ☒ Studierende/Stipendiat*Innen
- ☐ Andere:

Kategorien personenbezogener Daten, die verarbeitet werden

- ☐ Personenstammdaten (Name, Geburtsdatum)
- ☐ Adressdaten
- ☒ Kontakt- und Kommunikationsdaten (z.B. Telefon, E-Mail etc.)
- ☐ Qualifikationsdaten (z.B. Werdegänge, Lebensläufe, Qualifikationen etc.)
- ☐ Beschäftigendaten (Lohn- und Gehaltsdaten, Bankverbindung, Steuermerkmale etc.)
- ☐ Abrechnungs- und Zahlungsdaten
- ☒ Anwenderdaten (Browser-Daten, IP-Adressen, Cookies, Login-Name etc.)
- ☐ Bild- und Tonaufzeichnungsdaten
- ☐ Reise- und Standortdaten
- ☐ Besondere Kategorien von personenbezogenen Daten gem. Artikel 9 der Verordnung (EU) 2016/679 (z. B. Gesundheitsdaten, biometrische Daten, ethische, religiöse, politische, weltanschauliche Daten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person).
- ☐ Andere:

Anhang II – Liste der Unterauftragnehmer

- ☐ Der Auftragnehmer darf keinen seiner Verarbeitungsvorgänge, die er im Auftrag der Auftraggeberin gemäß diesen Klauseln durchführt, an einen Unterauftragnehmer untervergeben.

Die Auftraggeberin stimmt der Beauftragung folgender Unterauftragnehmer zu:

Name	Anschrift inkl. Land	Beschreibung der Verarbeitung (inkl. Gegenstand, Art und Dauer)	Bei Übermittlung von Daten an ein Drittland oder eine internationale Organisation: Wie ist die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 gewährleistet?

Anhang III – Technische und organisatorische Maßnahmen (TOM), einschließlich zur Gewährleistung der Sicherheit der Daten

Beschreibung der vom Auftragnehmer ergriffenen technischen und organisatorischen Sicherheitsmaßnahmen (einschließlich aller relevanten Zertifizierungen) zur Gewährleistung eines angemessenen Schutzniveaus unter Berücksichtigung der Art, des Umfangs, der Umstände und des Zwecks der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen.

Zur Darstellung kann die nachfolgende Checkliste verwendet werden, die eine Vielzahl möglicher technischer und organisatorischer Maßnahmen enthält. Die Checkliste ist nicht abschließend und muss vom Auftragnehmer für jeden Einzelfall, soweit notwendig, ergänzt werden. Um die konkrete Beschreibung sicherzustellen, müssen jeweils Erläuterungen eingefügt werden.

Die Darstellung und Beschreibung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen kann alternativ auch in einem separaten Dokument erfolgen.

1. Maßnahmen der Pseudonymisierung und Verschlüsselung personenbezogener Daten

- ☐ Pseudonymisierung von nicht mehr im Klartext benötigten personenbezogenen Daten
- ☐ Richtlinie zur Pseudonymisierung
- ☐ Verschlüsselung von Datenträgern
- ☐ Pseudonymisierung von Daten in Testsystemen
- ☐ Verschlüsselung von Webseiten (SSL)
- ☐ Verschlüsselung von Datenbanken
- ☐ E-Mail-Verschlüsselung (TLS 1.2 oder 1.3)
- ☐ Verschlüsselung von Passwörtern und Schlüsseln
- ☐ Verschlüsselung mobiler Geräte
- ☐ 

Erläuterung: 

2. Maßnahmen zur fortdauernden Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung

- ☐ Vertraulichkeitsvereinbarungen mit Mitarbeiter*innen
- ☐ Datenschutzverpflichtung der Mitarbeiter*innen
- ☐ Geheimhaltungsvereinbarung (NDA) mit Dritten
- ☐ Externer Speicher / Backup-Server
- ☐ Supportverträge mit Dritten
- ☐ Daten-Outsourcing-Vereinbarungen
- ☐ Nutzung zertifizierter Cloud-Anbieter
- ☐ Firewall
- ☐ Antivirenprogramm
- ☐ Regelmäßige Datensicherungen

- ☐ Redundante Systeme
- ☐ Überwachung von Systemen und Diensten
- ☐ RAID-Systeme
- ☐ Netzgebundener Speicher (NAS)
- ☐ Wartungsverträge
- ☐ Regelmäßige IT-Störfalltests
- ☐ Interne Speicherung von Kopien / Backups
- ☐ Unterbrechungsfreie Stromversorgung (UPS)
- ☐ Brand- und Rauchmeldeanlagen
- ☐ Geräte zur Überwachung von Temperaturen
- ☐ Ausrüstung zur Brandbekämpfung
- ☐ Alarmwarnung bei unberechtigtem Zugriff
- ☐ Load-Balancing
- ☐ 

Erläuterung: 

3. Maßnahmen zur Sicherstellung der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen

- ☐ Regelmäßige Backups des gesamten Systems
- ☐ Speicherung auf mehreren Systemen
- ☐ Datensicherungskonzept
- ☐ Regelmäßiger Test Backup/Recovery
- ☐ Hardware-Support- und Serviceverträge
- ☐ Notfallvorsorgekonzept
- ☐ Ausgelagerte Datensicherung
- ☐ Regelmäßige Schulung des IT-Personals
- ☐ 

Erläuterung: 

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

- ☐ Interne Kontrollen
- ☐ Auftragskontrolle (sorgfältige Auswahl der Auftragnehmer, eindeutige Vertragsgestaltung etc.)
- ☐ Regelmäßige Überprüfung der IT-Prozesse
- ☐ Regelmäßige Audits (z.B. durch den Datenschutzbeauftragten)
- ☐ Regelmäßige Überprüfung der Verfahren
- ☐ TOM-Audit durch den Datenschutzbeauftragten
- ☐ Regelmäßige Checks der Mitarbeiter*innen

- ☐ Durchführung von Datenschutz-Folgenabschätzungen
- ☐ Check Technikgestaltung / Voreinstellungen
- ☐ Datenschutzmanagementsystem / Datenschutzhandbuch
- ☐ 

Erläuterung: 

5. Maßnahmen zur Identifizierung und Autorisierung der Nutzer*innen

- ☐ Zwei-Faktor-Authentifizierung
- ☐ Authentifizierung mit Benutzername / Passwort
- ☐ Rollentrennung von Test- und Produktivsystem
- ☐ Regelmäßige Prüfung von Berechtigungen
- ☐ BIOS-Passwörter
- ☐ Berechtigungskonzept
- ☐ Richtlinie zur Verwaltung mobiler Geräte
- ☐ Benutzerprofile
- ☐ Passwort-Richtlinie
- ☐ Begrenzung der Anzahl der Admins
- ☐ Identifikation von neuen Mitarbeiter*innen
- ☐ Trennung der Benutzerrollen
- ☐ Automatische Verriegelungsmechanismen
- ☐ Identifikation Externer mit Ausweisen
- ☐ Verwaltung der Rechte durch einen Admin
- ☐ Unterscheidung zwischen Berechtigungen
- ☐ 

Erläuterung: 

6. Maßnahmen zum Schutz der Daten während der Übermittlung

- ☐ Einsatz von Verschlüsselungstechnologien
- ☐ Virtual Private Network (VPN)
- ☐ Protokollierung von Aktivitäten und Ereignissen
- ☐ Transport über eine private Cloud
- ☐ Dokumentation der Datenempfänger
- ☐ E-Mail-Verschlüsselung (TLS 1.2 oder 1.3)
- ☐ Verifizierung der Identität der Empfänger*innen
- ☐ Verwendung nicht-öffentlicher Laufwerke
- ☐ Physischer Transport: sichere Transportbehälter
- ☐ Sorgfältige Auswahl von Transportpersonal
- ☐ 

Erläuterung: **7. Maßnahmen zum Schutz der Daten während der Speicherung**

- ☐ Verschlüsselung von Datenträgern
- ☐ Datenklassifizierung
- ☐ Berechtigungskonzept
- ☐ Zugriffsbeschränkung
- ☐ Protokollierung von Aktionen und Ereignissen
- ☐ Sicherheitstüren
- ☐ Begrenzung der Anzahl der Administratoren
- ☐ Schlüsselkarte / RFID-Zugang
- ☐ Anonymisierung von Daten
- ☐ Pseudonymisierung von Daten
- ☐ Sichere Aufbewahrung von Datenträgern
- ☐ Firewall
- ☐ 

Erläuterung: **8. Maßnahmen zur Gewährleistung der physischen Sicherheit von Orten, an denen personenbezogene Daten verarbeitet werden**

- ☐ Alarmanlage
- ☐ Personenkontrolle / Pförtner
- ☐ Schutz von Gebäudeschächten
- ☐ Protokollierung der Besucher*innen
- ☐ Automatische Zugangskontrolle
- ☐ Sorgfältige Auswahl des Reinigungspersonals
- ☐ Sorgfältige Auswahl des Sicherheitspersonals
- ☐ Chipkarten, Transponder

- ☐ Schließsystem mit Codeschloss
- ☐ Pflicht zum Tragen von Berechtigungsausweisen
- ☐ Manuelles Schließsystem
- ☐ Zugriffskonzept
- ☐ Biometrische Zugangssperre
- ☐ Abschließbare Server-Schränke
- ☐ Videoüberwachung der Eingänge
- ☐ Türen mit einem Knauf an der Außenseite
- ☐ Lichtschranken / Bewegungsmelder
- ☐ Besucher*innen: Nur in Begleitung von Mitarbeiter*innen
- ☐ Sicherheitsschlösser
- ☐ Klingelanlage mit Kamera
- ☐ Verfahren zur Schlüsselausgabe
- ☐ 

Erläuterung: 

9. Maßnahmen zur Gewährleistung der Protokollierung von Ereignissen

- ☐ Einsatz einer automatischen Protokollierung
- ☐ Ereignisbericht-Erstellung
- ☐ Benachrichtigung mit Echtzeit-Alarm
- ☐ Protokollierung auf Applikationsebene
- ☐ Automatische Prüfung von Protokollen
- ☐ Synchronisation der Systemuhren
- ☐ Regelmäßige manuelle Überprüfung der Protokolle
- ☐ Automatische Konsolidierung von Ereignissen
- ☐ Protokolle werden in der Anwendung gespeichert und automatisch an einen anderen Ort gesendet
- ☐ 

Erläuterung: 

10. Maßnahmen zur Gewährleistung der Systemkonfiguration, einschließlich der Standardkonfiguration

- ☐ Konfigurationsmanagement-Richtlinie vorhanden
- ☐ Prozess zu Konfigurationsänderungen
- ☐ Datenschutzgerechte Voreinstellungen
- ☐ Check der Standardkonfigurationen
- ☐ Definition von Standardkonfigurationen
- ☐ Konfiguration durch Systemadministrator*in
- ☐ Protokollierung von Konfigurationsänderungen
- ☐ Regelmäßige Schulung der IT-Mitarbeiter*innen
- ☐ 

Erläuterung: 

11. Maßnahmen für die interne Governance und Verwaltung der IT und der IT-Sicherheit

- ☐ IT-Sicherheitsrichtlinie
- ☐ IT-Administrationsrichtlinie
- ☐ Regelmäßige Compliance-Audits / Überprüfungen
- ☐ IT-Anlagenverzeichnis
- ☐ Schulung der Mitarbeiter*innen zur Datensicherheit
- ☐ Regelmäßige Systemprüfung/ -bewertung
- ☐ IT-Team mit zugewiesenen Rollen / Verantwortlichkeiten
- ☐ Richtlinien für Ereignis-Management
- ☐ Risikobewertung und Maßnahmen zum Risikomanagement auf allen Stufen und Ebenen
- ☐ 

Erläuterung: 

12. Maßnahmen zur Zertifizierung/Qualitätssicherung von Prozessen und Produkte

- ☐ Einführung der ISO 9001 - Qualitätsmanagement
- ☐ Einführung der ISO 27001 - Informationssicherheitsmanagement
- ☐ Implementierung der ISO 27701 - Datenschutz-Informationsmanagement
- ☐ DS-GVO-Zertifizierung – Datenschutzmanagement
- ☐ Überblick über die für Produkte/Dienstleistungen/Prozesse geltenden Bestimmungen
- ☐ Identifikation von branchenspezifischen Standards
- ☐ Regelmäßige interne und/oder externe Audits
- ☐ Zuweisung von Audit-Verantwortlichkeiten an zertifizierte Expert*innen
- ☐ Regelmäßige Überprüfung auf neue Voraussetzungen und Erneuerung von Zertifikaten
- ☐ 

Erläuterung: **13. Maßnahmen zur Gewährleistung der Datenminimierung**

- ☐ Identifikation des Zwecks der Verarbeitung
- ☐ Bewertung des Zusammenhangs zwischen Verarbeitung und Zweck
- ☐ Beurteilung des Umfangs und der Qualität der verarbeiteten Daten in Bezug auf den Zweck
- ☐ Identifikation der geltenden Aufbewahrungsfristen
- ☐ Sichere Löschung der Daten nach Ablauf der Aufbewahrungsfrist
- ☐ 

Erläuterung: **14. Maßnahmen zur Gewährleistung der Datenqualität**

- ☐ Datenprofilierung und –klassifizierung
- ☐ Kontrolle eingehender oder neuer Daten
- ☐ Protokollierung der Eingabe/Änderung von Daten
- ☐ Rechtevergabe zur Dateneingabe
- ☐ Aufbewahrung von Protokollen
- ☐ Nachvollziehbarkeit der Benutzer*innen bei Eingabe, Änderung von Daten (keine Benutzergruppen)
- ☐ Vermeidung von doppelten Daten
- ☐ Identifizierung von Anforderungen an Daten
- ☐ Anwendung von Maßnahmen zur Datenqualität
- ☐ 

Erläuterung: 

15. Maßnahmen zur Gewährleistung einer begrenzten Vorratsdatenspeicherung

- ☐ Aufbewahrungsrichtlinie mit Rollen
- ☐ Trennung der Daten nach Aufbewahrungsfristen
- ☐ Regelmäßige Schulungen
- ☐ Regelmäßige Prüfung und Bewertung der gespeicherten Daten
- ☐ 

Erläuterung: 

16. Maßnahmen zur Gewährleistung der Rechenschaftspflicht

- ☐ Schulungen / Sensibilisierung
- ☐ Regelmäßige Kontrollen und Prüfungen
- ☐ Datenschutzteam vorhanden
- ☐ Anleitung und Unterstützung für Mitarbeiter*innen
- ☐ Angemessene Richtlinien zum Datenschutz
- ☐ Abschluss von Standardvertragsklauseln
- ☐ Vereinbarungen über gemeinsame Verantwortlichkeit
- ☐ Beantwortung von Anfragen betroffener Personen
- ☐ Transparenzdokument (Art. 13 / 14 DS-GVO)
- ☐ Sichere Datenlöschung
- ☐ Dokumentierte Datenschutzerklärung
- ☐ Auditberichte und Maßnahmen sind dokumentiert
- ☐ Ordnungsgemäße Einbeziehung des Datenschutzbeauftragten
- ☐ Spezifisches Einwilligungsverfahren / Aufbewahren von Einwilligungsprotokollen
- ☐ 

Erläuterung: 

17. Maßnahmen zur Ermöglichung der Datenübertragbarkeit und zur Gewährleistung der Löschung

- ☐ Speicherung in einem strukturierten Format
- ☐ Überwachung gesetzlicher Fristen
- ☐ Übertragung per End-to-End-Verschlüsselung
- ☐ Einhaltung von Aufbewahrungsfristen
- ☐ Ermöglichung der Datenübertragbarkeit
- ☐ Umgang mit Betroffenenrechten gemäß Kapitel 3 der Verordnung (EU) 2016/679
- ☐ Sichere Datenlöschung gewährleistet
- ☐ Sichere Datenträgervernichtung gewährleistet
- ☐ 

Erläuterung: 