

# Vertrag über die Verarbeitung personenbezogener Daten im Auftrag

auf der Grundlage von Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679

## **ABSCHNITT I**

### ***Klausel 1***

#### ***Zweck und Anwendungsbereich***

- (a) Mit diesem Vertrag über die Verarbeitung personenbezogener Daten im Auftrag (im Folgenden „AVV“ oder „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, DSGVO) sichergestellt werden.
- (b) Die in Anhang I aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 zu gewährleisten.
- (c) Diese AVV gilt für die Verarbeitung personenbezogener Daten gemäß Anhang II.
- (d) Die Anhänge I bis V<sup>1</sup> sind Bestandteil der Klauseln.
- (e) Diese AVV gilt unbeschadet der Verpflichtungen, denen der Verantwortliche 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.

### ***Klausel 2***

#### ***Unabänderbarkeit der Klauseln***

*Diese Klausel wurde absichtlich leer gelassen*

### ***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.

---

<sup>1</sup> Die Anhänge I bis IV entsprechen den vorgesehenen Anhängen der Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 der von der EU-Kommission erlassenen Verordnung (EU) 2016/679. Anhang V umfasst Regelungen, die insbesondere dazu dienen, das Schutzniveau zugunsten der betroffenen Person zu erhöhen, und sofern relevant, dem deutschen Telekommunikations- und/oder Telemedienrecht zu entsprechen.

- (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***

##### ***Kopplungsklausel***

*Diese Klausel wurde absichtlich leer gelassen*

### **ABSCHNITT II** **PFLICHTEN DER PARTEIEN**

#### ***Klausel 6***

##### ***Beschreibung der Verarbeitung***

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

#### ***Klausel 7***

##### ***Pflichten der Parteien***

#### **7.1. Weisungen**

- (a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.
- (b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

## 7.2. Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang II genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

## 7.3. Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragsverarbeiter nur für die in Anhang II angegebene Dauer verarbeitet.

## 7.4. Sicherheit der Verarbeitung

- (a) Der Auftragsverarbeiter 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) Der Auftragsverarbeiter 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 Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

## 7.5. 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 Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

## 7.6. Dokumentation und Einhaltung der Klauseln

- (a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.
- (b) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.
- (c) Der Auftragsverarbeiter stellt dem Verantwortlichen 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 des Verantwortlichen gestattet der Auftragsverarbeiter 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 der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.

- (d) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.
- (e) Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

### **7.7. Einsatz von Unterauftragsverarbeitern**

- (a) Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens 14 Tage im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.
- (b) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 unterliegt.
- (c) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen 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 Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.
- (d) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten, gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.
- (e) Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

### **7.8. Internationale Datenübermittlungen**

- (a) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 im Einklang stehen.
- (b) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 7.7 für die Durchführung bestimmter

Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter 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 8***

#### ***Unterstützung des Verantwortlichen***

- (a) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.
- (b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.
- (c) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8 Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen 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(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche 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 Auftragsverarbeiter den Verantwortlichen 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 des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

### ***Klausel 9***

#### ***Meldung von Verletzungen des Schutzes personenbezogener Daten***

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 nachkommen kann, wobei der

Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

### **9.1 Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten**

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

- (a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen 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 des Verantwortlichen 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 vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und sofern nicht alle diese Informationen zur selben 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.

### **9.2 Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten**

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen 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 sofern nicht alle diese Informationen zur selben 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 Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679 zu unterstützen.

### **ABSCHNITT III** **SCHLUSSBESTIMMUNGEN**

#### ***Klausel 10***

##### ***Verstöße gegen die Klauseln und Beendigung des Vertrags***

- (a) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.
- (b) Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn
  - (1) der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter 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 Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 nicht erfüllt;
  - (3) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 zum Gegenstand hat, nicht nachkommt.
- (c) Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe b verstoßen.
- (d) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen 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 Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

Die nachstehend aufgeführten Anhänge sind Bestandteil dieser Klauseln:

- **Anhang I: "LISTE DER PARTEIEN"**
- **Anhang II: "BESCHREIBUNG DER VERARBEITUNG"**
- **Anhang III "TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN, EINSCHLIEßLICH ZUR GEWÄHRLEISTUNG DER DATENSICHERHEIT "**
- **Anhang IV: "LISTE DER UNTERAUFTRAGSVERARBEITER"**
- **Anhang V "ERGÄNZENDE REGELUNGEN ZUM AVV"**

## ANHANG I

### Liste der Parteien

#### Verantwortliche(r):

1.1	<b>Name und Anschrift</b>	Gemäß Kundenangaben innerhalb des Vertragsformulars
1.2	<b>Kontakt zum Verantwortlichen</b>	Gemäß Kundenangaben innerhalb des Vertragsformulars
1.3	<b>E-Mail-Adresse zur Meldung von Datenschutzvorfällen</b>	Gemäß Kundenangaben innerhalb des Vertragsformulars

#### Auftragsverarbeiter:

1.4	<b>Name und Anschrift</b>	Telefónica Germany GmbH & Co. OHG, Georg-Brauchle-Ring 50 80992 München Deutschland
1.5	<b>Kontaktdaten des/der Datenschutzbeauftragten</b>	<a href="mailto:datenschutz@telefonica.com">datenschutz@telefonica.com</a>

## ANHANG II

### BESCHREIBUNG DER VERARBEITUNG

2.1.	<b>Beschreibung der konkreten Datenverarbeitung (Gegenstand, Art und Umfang)</b>	<p>Der Auftragsverarbeiter führt im Namen des Verantwortlichen folgende Verarbeitungstätigkeiten durch:</p> <p>Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Vermittlung eines direkten Vertragsverhältnisses mit Netskope und erbringt für den Verantwortlichen Managed Services für Security Service Edge (SSE)-Lizenznehmer des Herstellers Netskope.</p> <p>Während des Vertragsverhältnisses werden die folgenden Verarbeitungstätigkeiten vom Auftragsverarbeiter - hauptsächlich über seine Unterauftragsverarbeiter - durchgeführt:</p> <ul style="list-style-type: none"> <li>- Weiterleitung von Informationen des Verantwortlichen an Netskope oder dessen Partner zum Zwecke der Erstellung eines Vertragsangebots zwischen Netskope und dem Verantwortlichen.</li> <li>- Zugang zu den Kontaktdaten der Mitarbeiter des Verantwortlichen, um die Konfiguration der Sicherheitsrichtlinien sowie andere Konfigurationsmaßnahmen vorzunehmen, sofern eine entsprechende Anfrage des Kunden vorliegt (auf der Grundlage eines Tickets).</li> <li>- Zugang zu den Kontaktdaten der Mitarbeiter des Verantwortlichen, um die Inbetriebnahme des SSE-Plattformkonto des Verantwortlichen von Netskope aus zu ermöglichen.</li> <li>- Benutzerinstallationen im SSE-Plattformkonto des Verantwortlichen; Benutzer sind Mitarbeiter des Verantwortlichen.</li> <li>- Fernzugriff auf das SSE-Plattformkonto des Verantwortlichen für             <ul style="list-style-type: none"> <li>o Verwaltung der von den Cybersicherheitsdiensten generierten Warnungen (optional, auf Anfrage).</li> <li>o Durchführung einer Analyse eines eventuell aufgetretenen Vorfalls und Einleitung geeigneter Maßnahmen (optional, auf Anfrage).</li> <li>o Bereitstellung von Support bei Problemen mit dem Konto.</li> <li>o Monatlicher Bericht mit Kundentickets (optional, auf Anfrage).</li> </ul> </li> <li>- Kundenbetreuung und Unterstützung bei der Kommunikation zwischen dem Verantwortlichen und Netskope.</li> </ul> <p>Die Kontaktdaten des Verantwortlichen werden dem Auftragsverarbeiter von dem Verantwortlichen über ein Formular und/oder über Support-Tickets zur Verfügung gestellt, um die eigentlichen Dienste bereitzustellen und den Support zu erleichtern. Der Verantwortliche wird eine direkte vertragliche Beziehung mit Netskope für die Lizenzierung des Security Service Edge eingehen.</p> <p>Um den Dienst im Namen des Verantwortlichen zu verwalten (u.a. Sicherheitsrichtlinien festzulegen, Aktivitäten zu überwachen und Berichte zu erstellen) ist ein Fernzugriff auf die im SSE-Plattformkonto des Verantwortlichen gespeicherten Informationen innerhalb der Netskope-Plattform erforderlich.</p> <p>Diese Tätigkeiten werden durchgeführt  <input checked="" type="checkbox"/> in Systemen, die vom Verantwortlichen und Auftragsverarbeiter (inkl. dessen Unterauftragsverarbeitern) bereitgestellt werden</p> <p>Der Auftragsverarbeiter wird hierbei Zugang zu personenbezogenen Daten des Verantwortlichen nur in dem Umfang nutzen, als dies für die in den folgenden Abschnitten dieses Anhangs beschriebenen Zwecke erforderlich ist.</p>
2.2.	<b>Hauptvertrag (Purchase Order-/ Vertragsbezeichnung: Geplante Dauer des Auftrags)</b>	<p>Gemäß des Vertragsformulars.</p> <p><input checked="" type="checkbox"/> befristet bis: Beendigung des o.g. Hauptvertrages</p>

2.3	Bitte hier angeben, welchem <b>Zweck</b> die Tätigkeit des Auftragsverarbeiters dient	<b>1. Zwecke bezüglich IT-Leistungen</b> <input checked="" type="checkbox"/> Verwaltung von Zugangs-/ Zugriffsrechten auf Informations- und Kommunikationstechnik und Unternehmensnetzwerk <input checked="" type="checkbox"/> Wartung/ Support (maintenance)  <b>2. Sonstige Zwecke</b> <input checked="" type="checkbox"/> Sonstiges: Vertragsvermittlung mit Netskope
2.4	Bitte hier die <b>Datenkategorien</b> angeben, die durch den Auftragsverarbeiter verarbeitet werden	<b>1. Sonstige Datenarten</b> <input checked="" type="checkbox"/> Sonstiges: Die Kategorien personenbezogener Daten werden durch den Verantwortlichen nach eigenem Ermessen festgelegt und können unter anderem Folgendes umfassen: Namen, Beruf, Standort, Arbeitgeber, Beziehung zur Organisation, E-Mail-Adresse, Telefonnummer, IP-Adresse, Active Directory, Benutzername, Organisationseinheit, Benutzerzuordnung im Active Directory (falls konfiguriert), Cloud-Anwendung, auf die der Benutzer zugreift, vom Benutzer durchgeführte Aktivität. Kontaktinformationen: E-Mail-Adresse für die Benachrichtigung über Support Tickets.
2.5	Die Daten welcher <b>betroffenen Personen</b> werden durch den Auftragsverarbeiter verarbeitet?	<input checked="" type="checkbox"/> Potenzielle Kund:innen/ Interessent:innen <input checked="" type="checkbox"/> Beschäftigte (z.B. Mitarbeiter:innen, Praktikant:innen, Auszubildende)
2.6	Werden bei den vom Auftragsverarbeiter erbrachten Dienstleistungen <b>sensible Daten</b> gemäß Ziffer 7.5 verarbeitet?	<input checked="" type="checkbox"/> Nein
2.7	Bitte geben Sie die <b>Kategorien der Datenempfänger</b> an. Übermittelt der Auftragsverarbeiter die Daten im Auftrag des Verantwortlichen an einen Dritten oder einen Auftragsverarbeiter?	<input checked="" type="checkbox"/> Unterauftragsverarbeiter des Auftragsverarbeiters (gilt auch für Konzernunternehmen von Auftragsverarbeitern; Beschreibung der (Unter-) Verarbeitung in <b>Anhang IV</b> )  <input checked="" type="checkbox"/> Übermittlung an Dritte ( <b>nicht</b> Unterauftragsverarbeiter): Netskope und ihre Distributoren
2.8	Bitte geben Sie alle Standorte an, an denen die Daten des Verantwortlichen <b>gespeichert</b> sind.	<input checked="" type="checkbox"/> Deutschland <input checked="" type="checkbox"/> EU/EWR abgesehen von Deutschland
2.9	Bitte geben Sie alle Standorte an, von denen aus auf die Daten des Verantwortlichen wie vorgesehen <b>zugriffen</b> wird.	<input checked="" type="checkbox"/> Deutschland <input checked="" type="checkbox"/> EU/EWR abgesehen von Deutschland
2.10	Bitte ggf. geltende <b>gesetzliche Verpflichtungen zur Verarbeitung</b> der für den Verantwortlichen verarbeiteten Daten angeben.	Bestehen zum Zeitpunkt des Abschlusses dieses Vertrages entsprechende Verpflichtungen nach dem Recht der Europäischen Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, die Daten des Verantwortlichen zu verarbeiten (Art. 28 Abs. 3 S. 2 lit. a DSGVO)?  <input checked="" type="checkbox"/> Nein

2.11	Bitte Vorgaben für die <b>Datenlöschung</b> machen.	<p>Die Daten des Verantwortlichen (insbesondere Bestands-/ Verkehrs-/ Inhalts- und Mitarbeiterdaten) sind zu löschen, wenn sie für die Durchführung des Auftrags nicht mehr erforderlich sind, es sei denn es liegt eine abweichende Weisung des Verantwortlichen vor. Die Löschung von Verkehrsdaten hat entsprechend den rechtlichen Anforderungen aus dem "Leitfaden des BfDI und der BNetzA für eine datenschutzgerechte Speicherung von Verkehrsdaten" zu erfolgen.</p> <p>Eine Datenspeicherung erfolgt ausschließlich in den Systemen des Verantwortlichen:  <input checked="" type="checkbox"/> <b>Nein:</b></p> <p>Die personenbezogenen Daten des Verantwortlichen sind, soweit keine entgegenstehende Einzelweisung erfolgt oder eine gesetzliche oder anderweitige Aufbewahrungspflicht entgegensteht, nach Weitergabe an den Verantwortlichen innerhalb von 30 Tagen zu löschen. Spätestens 30 Tage nach Vertragsbeendigung werden die personenbezogenen Daten nach Weisung des Verantwortlichen gelöscht bzw. an den Verantwortlichen herausgegeben und die Kopien gelöscht. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind. Der Auftragsverarbeiter vernichtet diese Datensätze ohne Aufforderung des Verantwortlichen mit Ablauf der Aufbewahrungspflichten bzw. mit Wegfall der Notwendigkeit der Datenspeicherung zu Sicherheitszwecken.</p> <p>Soweit nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur (weiteren) Speicherung von den im Auftrag gespeicherten Daten einer Löschung entgegensteht, bitte Verpflichtung inkl. Rechtsgrundlage und Frist angeben: Rechnungen mindestens 10 Jahre § 14 b UStG, § 147 AO</p> <p>Wird eine Archivierung <b>für den Verantwortlichen</b> durchgeführt?  <input checked="" type="checkbox"/> <b>Nein</b></p>
------	---	--

**ANHANG III - Technische und organisatorische Maßnahmen, einschließlich zur Gewährleistung der Sicherheit der Daten**

1.	Sind <b>Best Practice Sicherheitsmaßnahmen</b> (z.B. Sicherheitskonzept nach Art. 32 DS-GVO, internationale Standards) berücksichtigt worden?	<input checked="" type="checkbox"/> Implementierte Sicherheitsmaßnahmen sind immer auf dem Stand der Technik gehalten
2.	Sind Maßnahmen zur <b>Pseudonymisierung</b> personenbezogener Daten ergriffen worden?	<input checked="" type="checkbox"/> Nein, weil <i>(bitte begründen)</i> : zur Leistungserbringung durch den Verantwortlichen Klardaten benötigt werden.
3.	Sind Maßnahmen zur räumlichen <b>Zutrittskontrolle</b> ergriffen worden, die es Unbefugten verwehren, sich den Systemen, Datenverarbeitungsanlagen oder Verfahren physisch zu nähern, mit denen personenbezogene Daten verarbeitet werden?	<input checked="" type="checkbox"/> Ja  Maßnahmen: <input checked="" type="checkbox"/> Konzept Sicherheitszonen <input checked="" type="checkbox"/> Schlüsselverwaltung / Dokumentation der Schlüsselübergabe <input checked="" type="checkbox"/> Zutrittskontrollsystem, z.B. Ausweisleser (Magnet-/ Chipkarten) <input checked="" type="checkbox"/> Werkschutz / Pförtner <input checked="" type="checkbox"/> Sicherheitstüren / -fenster <input checked="" type="checkbox"/> Türsicherungen (elektrische Türöffner, Zahlenschloss, etc.) <input checked="" type="checkbox"/> Alarmanlage <input checked="" type="checkbox"/> Videoüberwachung <input checked="" type="checkbox"/> Spezielle Schutzvorkehrungen des Serverraums
4.	Sind Maßnahmen zur <b>Zugangskontrolle</b> ergriffen worden, die gewährleisten, dass ein Zugang durch Unbefugte auf Datenverarbeitungssysteme verhindert wird?	<input checked="" type="checkbox"/> Ja  Maßnahmen: <input checked="" type="checkbox"/> Benutzer haben einen eindeutigen persönlichen Bezeichner <input checked="" type="checkbox"/> Benutzerkennungen werden, wenn die Benutzer das Unternehmen verlassen haben, gelöscht oder deaktiviert <input checked="" type="checkbox"/> Passwörter werden grundsätzlich nicht im Klartext gespeichert oder unverschlüsselt übertragen <input checked="" type="checkbox"/> Sichere Passwortverfahren <input checked="" type="checkbox"/> Sichere Erzeugung und Übermittlung von Initial- und Reset-Passwörtern <input checked="" type="checkbox"/> Zwei-Faktor-Authentifizierung für kritische Anwendungen <input checked="" type="checkbox"/> Automatische Sperrung der Clients nach Zeitablauf ohne Useraktivität (z.B. passwortgeschützter Bildschirmschoner) <input checked="" type="checkbox"/> sichere Verwaltung und Verwendung von digitalem Schlüsselmaterial (z.B.: digitale Zertifikate, Token, etc.) <input checked="" type="checkbox"/> Regelmäßige Softwareaktualisierung / Patching (Patchmanagement) <input checked="" type="checkbox"/> Netzwerksegmentierung <input checked="" type="checkbox"/> Firewall, IDS/IPS
5.	Sind Maßnahmen zur <b>Zugriffskontrolle</b> ergriffen worden, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können?	<input checked="" type="checkbox"/> Ja  Maßnahmen:  <input checked="" type="checkbox"/> Angemessene Berechtigungskonzepte inkl. der Dokumentation von: <input checked="" type="checkbox"/> Verantwortlichkeiten <input checked="" type="checkbox"/> Aufgabenbezogenen Profile und Rollen <input checked="" type="checkbox"/> Rollenkonzept(e)  <input checked="" type="checkbox"/> Benutzermanagementprozess inkl. Genehmigungsverfahren <input checked="" type="checkbox"/> Regelmäßige Prüfung der Aktualität von Zugriffsrechten (Rezertifizierung)

6.	Sind Maßnahmen zur <b>Weitergabekontrolle</b> ergriffen worden, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist?	<input checked="" type="checkbox"/> Ja  Maßnahmen: <input checked="" type="checkbox"/> Gesichertes WLAN <input checked="" type="checkbox"/> SSL-/TLS-Verschlüsselung <input checked="" type="checkbox"/> Verwaltung kryptographischer Schlüssel <input checked="" type="checkbox"/> Richtlinie für eine aufgeräumte Arbeitsumgebung (z.B. Clean-Desk-Policy)
7.	Sind Maßnahmen zur <b>Eingabekontrolle</b> ergriffen worden, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind?	<input checked="" type="checkbox"/> Ja  Maßnahmen: <input checked="" type="checkbox"/> Berechtigungskonzepte vorhanden, inkl. der Dokumentation von: <input checked="" type="checkbox"/> Funktionalen Verantwortlichkeiten <input checked="" type="checkbox"/> Angemessener Funktionstrennung
8.	Sind Maßnahmen zur <b>Auftragskontrolle</b> ergriffen worden, die sicherstellen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden können?	<input checked="" type="checkbox"/> Ja  Maßnahmen: <input checked="" type="checkbox"/> Verbindliche Sicherheitsleitlinien inkl. Verpflichtungen der Mitarbeiter <input checked="" type="checkbox"/> Schulungen aller zugriffsberechtigten Mitarbeiter <input checked="" type="checkbox"/> Betriebshandbücher für den sicheren Betrieb <input checked="" type="checkbox"/> Regelmäßige Datenschutzaudits des betrieblichen Datenschutzbeauftragten <input checked="" type="checkbox"/> Prüfungsplanung für interne und externe Audits <input checked="" type="checkbox"/> Nutzung eines risikoorientierten Auditansatzes <input checked="" type="checkbox"/> Monitoring & Reporting über neu identifizierte Risiken / Schwachstellen <input checked="" type="checkbox"/> IT-Change Management Prozess <input checked="" type="checkbox"/> Verbot der Installation nicht freigegebener Software / Applikationen auf den Endgeräten <input checked="" type="checkbox"/> Trennung von Entwicklungs- und Produktivsystemen inkl. geregelter Transportprozess (production take over) <input checked="" type="checkbox"/> Genehmigungs- und Freigabeverfahren
9.	Sind Maßnahmen zur <b>Verfügbarkeitskontrolle</b> ergriffen worden, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind bzw. zügig wiederhergestellt werden können?	<input checked="" type="checkbox"/> Ja  Maßnahmen: <input checked="" type="checkbox"/> Business Continuity Strategie und Management <input checked="" type="checkbox"/> Service Level Agreements (SLAs) mit Dienstleistern <input checked="" type="checkbox"/> Backup Verfahren <input checked="" type="checkbox"/> Viren-/Schadcodeschutz <input checked="" type="checkbox"/> Schutz der relevanten Infrastruktur gegen Defekte durch äußere Einflüsse <input checked="" type="checkbox"/> Pläne für Ausfall / Notfall / Wiederanlauf etc. (einzelner Komponenten)
10.	Sind Maßnahmen zur Einhaltung des <b>Trennungsgebots</b> ergriffen worden, die gewährleisten, dass Daten, die zu unterschiedlichen Zwecken	<input checked="" type="checkbox"/> Ja  Maßnahmen: <input checked="" type="checkbox"/> Trennung durch Zugriffsregelungen

	erhoben werden, getrennt verarbeitet (z.B. gelöscht) werden können.	
11.	Sind Maßnahmen und Verantwortlichkeiten für den <b>Umgang mit Informationssicherheitsvorfällen und Krisensituationen</b> definiert worden?	<input checked="" type="checkbox"/> Ja  <b>Maßnahmen:</b> <input checked="" type="checkbox"/> Managementprozess für Security Incidents <input checked="" type="checkbox"/> Managementprozess für datenschutzrelevante Incidents <input checked="" type="checkbox"/> Definition der Sicherheitsanforderungen in Krisensituation / im Notfall
12.	Sind Maßnahmen für <b>Logging</b> in den relevanten Bereichen ergriffen worden?	<input checked="" type="checkbox"/> Ja  <input checked="" type="checkbox"/> Es existiert ein dokumentiertes Loggingkonzept <input checked="" type="checkbox"/> Nutzung von Sicherheits-/Protokollierungssoftware <input checked="" type="checkbox"/> Die Log-Systeme beziehen sich auf eine einzige Zeitquelle <input checked="" type="checkbox"/> Verarbeitung der Daten in Übereinstimmung mit geltenden gesetzlichen Bestimmungen für die Informationssicherheit <input checked="" type="checkbox"/> Logs sind gegen unberechtigten Zugriff geschützt (Vertraulichkeit) <input checked="" type="checkbox"/> Logs sind vor unberechtigter Veränderung geschützt (Integrität)  <b>Eingabekontrolle</b> <input checked="" type="checkbox"/> Systemseitiges Logging von Eingaben  <b>Verfügbarkeitskontrolle</b> <input checked="" type="checkbox"/> Logging der Verfügbarkeit <input checked="" type="checkbox"/> Regelmäßige Überwachung der Systeme und Logfiles  <b>Zutrittskontrolle</b> <input checked="" type="checkbox"/> Logging der Zutritte <input checked="" type="checkbox"/> Regelmäßiges Monitoring von Zutritten  <b>Zugangskontrolle</b> <input checked="" type="checkbox"/> Logging der Zugänge  <b>Zugriffskontrolle</b> <input checked="" type="checkbox"/> Logging der Zugriffe <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> lesend</li> <li><input checked="" type="checkbox"/> schreibend</li> </ul>

### ANHANG IV – LISTE DER UNTERAUFTRAGSVERARBEITER

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

*Ja => Die folgende Tabelle ist auszufüllen.* Andere Unterauftragsverarbeiter, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten oder auf diese zugreifen können und nicht in der Tabelle aufgeführt sind, wurden vom Auftragsverarbeiter **nicht** beauftragt.

Angabe des Unterauftragsverarbeiters	Beschreibung der Verarbeitung	Bestehen Verträge zur Auftragsverarbeitung zwischen dem Auftragsverarbeiter und Unterauftragsverarbeiter (Art. 28 Abs. 4 DSGVO)?	Findet eine Übermittlung oder ein Zugriff auf die Daten des Verantwortlichen In/aus Drittländern (außerhalb der EU/ des EWR) statt?	Bitte nur im Falle eines Datenzugriffs aus / einer Datenübermittlung in ein Drittland beantworten: Hat der Auftragsverarbeiter gesetzlich vorgeschriebene Garantien und, soweit relevant, Supplementary Measures (vgl. EDPB, Empfehlungen 01/2020 <sup>2</sup> ) gemäß Kapitel V der DSGVO vorgesehen?
<p>Name/Firma: Telefónica Cybersecurity &amp; Cloud Tech Deutschland GmbH Adresse: Adalperostrasse 82-86, 85737 Ismaning</p> <p>Name, Position und Kontaktdaten der Kontaktperson: Klaus Luehr klaus.luehr@telefonica.com</p> <p><b>Ort der Speicherung/ des bestimmungsgemäßen Zugriffs auf die im Auftrag verarbeiteten Daten</b> Ronda de la Comunicación, s/n, Edificio Oeste 1, 28050, Madrid, Spanien</p>	<p>Der Unterauftragsverarbeiter unterstützt den Auftragsverarbeiter bei den unter Anhang 2 Punkt 2.1 aufgeführten Verarbeitungen.</p>	<p><input checked="" type="checkbox"/> Ja, Vereinbarungen gemäß Art. 28 Abs. 4 DSGVO bestehen</p>	<p><input checked="" type="checkbox"/> Nein, eine Zugriffsmöglichkeit auf diese Daten von außerhalb der EU/ des EWR ist technisch ausgeschlossen.</p>	

<sup>2</sup> Empfehlungen 01/2020 zu “Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene” des European Data Protection Board (EDPB), angenommen am 18. Juni 2021

## **ANHANG V ERGÄNZENDE REGELUNGEN ZUM AVV**

Anhang V umfasst Regelungen, die insbesondere dazu dienen, das Schutzniveau zugunsten der betroffenen Person zu erhöhen, und die generischen Bedingungen zu Dauer und Verletzungen des Vertrags zu konkretisieren.

### **1. Vertragsdauer und -beendigung**

- 1.1 Unbeschadet Klausel 10 (b) endet diese AVV sechs (6) Monate nach Beendigung einer diesem Vertrag zugrundeliegenden Beauftragung (Hauptvertrag), ohne dass es einer separaten Kündigung dieses Vertrages bedarf.

Sofern kein Hauptvertrag geschlossen wurde, wird dieser Vertrag auf unbestimmte Zeit geschlossen. Die Kündigungsfrist beträgt in diesem Fall drei (3) Monate.

Das Recht auf außerordentliche Kündigung nach den gesetzlichen Bestimmungen bleibt unberührt.

- 1.2 Die Verpflichtungen gemäß den Klauseln 7 bis 10 (a) der AVV bleiben über das Datum der Beendigung der Vereinbarung hinaus bis zu dem Zeitpunkt in Kraft, an dem die vollständige Löschung/Rückgabe der entsprechenden personenbezogenen Daten durch den Auftragsverarbeiter an den für die Verarbeitung Verantwortlichen bestätigt wurde.

### **2. Remote Access/Homeoffice**

Die Verarbeitung von personenbezogenen Daten des Verantwortlichen außerhalb der Betriebsstätte des Auftragsverarbeiters (z.B. im Homeoffice oder bei sonstigem Remote-Zugriff) ist zulässig. Der Auftragsverarbeiter stellt sicher, dass auch in diesem Fall die erforderlichen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO ergriffen und dokumentiert werden, die den Besonderheiten dieser Verarbeitungssituationen in angemessener Weise Rechnung tragen und insbesondere auch eine ausreichende Kontrolle der Datenverarbeitung ermöglicht.

### **3. Einspruch gegen Unterauftragsverarbeiter**

Soweit der Verantwortliche Einspruch innerhalb der unter Klausel 7.7 (a) genannten Frist gegen die Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters erhebt, wird der Verantwortliche dem Auftragsverarbeiter einen Grund für den Einspruch mitteilen. Aus der Begründung muss hervorgehen, warum der Unterauftragsverarbeiter nach Auffassung des Verantwortlichen keine hinreichende Garantie für eine Verarbeitung im Einklang mit den Anforderungen der DSGVO und diesem AVV sowie den Schutz der Rechte der betroffenen Person gewährleistet. Soweit fristgemäß Einspruch eingelegt wird, werden sich der Verantwortliche und der Auftragsverarbeiter innerhalb einer Frist von [...] untereinander abstimmen, inwieweit die Einbeziehung des Unterauftragsverarbeiters nach Vorgaben des Verantwortlichen ausgeschlossen oder eingeschränkt werden kann und er seinen Einspruch zurückzieht. Sollte der Verantwortliche an seiner Einschätzung und dem Einspruch festhalten, werden die Parteien abstimmen, inwieweit der Vertrag – unter Berücksichtigung der einschlägigen Kündigungsfristen – zu beenden ist.

### **4. Vertragsstrafe, Haftung**

Die Haftungs- und Schadensersatzvereinbarungen aus dem Hauptvertrag, soweit sie auf der Verletzung einer wesentlichen Vertragspflicht beruhen, finden auf diesen Vertrag Anwendung. Wesentliche Vertragspflichten sind Pflichten, deren Erfüllung die ordnungsgemäße Durchführung des Vertrages überhaupt erst ermöglicht, deren Verletzung die Erreichung des Vertragszwecks gefährdet

und auf deren Einhaltung der Verantwortliche regelmäßig vertrauen darf. Die Haftung des Auftragsverarbeiters gegenüber dem Verantwortlichen ist allerdings wie folgt limitiert auf: Vorhersehbare, vertragstypische Schäden, jedoch nur bis zu einer Höhe von 100 % des auf den Verantwortlichen entfallenen jährlichen Volumens des Hauptvertrags.

## **5. Internationale Datenübermittlungen**

Zur Gewährleistung von geeigneten Garantien zum Schutz der Übermittlung und der Verarbeitung personenbezogener Daten außerhalb der EU erfolgt die Datenübermittlung an und Datenverarbeitung durch die in Anlage IV aufgeführten weiteren Auftragsverarbeiter außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums auf Basis geeigneter Garantien nach Art. 46 ff. DSGVO, insbesondere durch den Abschluss von Standarddatenschutzklauseln nach Art. 46 Abs. 2 lit. c DSGVO.

## **6. Sonstige Bestimmungen**

- 6.1 Änderungen und Ergänzungen dieses Vertrags und aller seiner Bestandteile bedürfen einer Vereinbarung in Schriftform und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieses Vertrags handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
- 6.2 Sollte eine Bestimmung dieses Vertrages unwirksam sein oder werden, oder eine an sich notwendige Regelung nicht enthalten sein, so wird dadurch die Wirksamkeit der übrigen Bestimmungen dieses Vertrages nicht berührt. Anstelle der unwirksamen Bestimmung oder zur Ausfüllung der Regelungslücke gilt eine rechtlich zulässige Regelung, die so weit wie möglich dem entspricht, was die Parteien gewollt haben oder nach Sinn und Zweck dieses Vertrages gewollt hätten, wenn sie die Regelungslücke erkannt hätten.
- 6.3 Soweit rechtlich zulässig und in einem ggf. geschlossenen Hauptvertrag nichts Abweichendes bestimmt ist, gilt deutsches Recht und der Gerichtsstand München.