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

Diese Klauseln, einschließlich seiner Anhänge, konkretisieren die datenschutzrechtlichen Verpflichtungen, die sich aus der Beauftragung der Telefónica Germany GmbH & Co. OHG, Georg-Brauchle-Ring 50, 80992 München im Rahmen der diesem Vertrag zu Grunde liegenden O2 Business „Mobile Device Management (MDM)“ Leistung („Hauptvertrag“) ergeben. Für diesen Annex gelten die Begriffsbestimmungen 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“), sofern nichts Abweichendes bestimmt wurde.

Im Rahmen der Nutzung des von der Telefónica Germany GmbH & Co. OHG bereitgestellten Dienst O_2 Business „Mobile Device Management (MDM)““ werden regelmäßig personenbezogene Daten verarbeitet. Sie sind gemäß gesetzlicher Regelungen dazu verpflichtet, einen Vertrag über die Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 DSGVO (nachfolgend „AVV“ oder „Klauseln“ genannt) abzuschließen.

Vertragspartner sind die Telefónica Germany GmbH & Co. OHG, Georg-Brauchle-Ring 50, 80992 München (Auftragsverarbeiter i.S.d. Art. 4 Nr. 8 DSGVO) und der Kunde (nachfolgend gemeinsam die „Parteien“ genannt). "Kunde" im Sinne dieser Klauseln bezeichnet das Unternehmen, welches den Hauptvertrag im eigenen Namen und, soweit nach den geltenden Datenschutzgesetzen und -vorschriften erforderlich, im Namen und im Auftrag seiner Unternehmensgruppe unterzeichnet hat. Dieser Vertrag kommt mit Unterzeichnung des Hauptvertrages durch die Parteien zustande. Der Kunde ist für die Datenverarbeitung im Zusammenhang mit O_2 „Mobile Device Management (MDM)““ i.S.d. Art. 4 Nr. 7 DSGVO verantwortlich.

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[1] 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.

(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.

[1] 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.

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 personenbezogene 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 darf keinen seiner Verarbeitungsvorgänge, die er im Auftrag des Verantwortlichen gemäß diesen Klauseln durchführt, ohne vorherige gesonderte schriftliche Genehmigung des Verantwortlichen an einen Unterauftragsverarbeiter untervergeben. Der Auftragsverarbeiter reicht den Antrag auf die gesonderte Genehmigung mindestens 14 Tagen vor der Beauftragung des betreffenden Unterauftragsverarbeiters zusammen mit den Informationen ein, die der Verantwortliche benötigt, um über die Genehmigung zu entscheiden. Die Liste der vom Verantwortlichen genehmigten Unterauftragsverarbeiter findet sich in Anhang IV. Die Parteien halten Anhang IV jeweils auf dem neuesten Stand.

(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.

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 ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER PERSONENBEZOGENEN DATEN"
- **Anhang IV**: "LISTE DER UNTERAUFTRAGSVERARBEITER"
- **Anhang V** "ERGÄNZENDE REGELUNGEN ZUM AVV"

ANHANG I

Liste der Parteien

Verantwortliche(r):

1.1	**Name und Anschrift**	Gemäß Kundenangaben innerhalb des Hauptvertrages
1.2	**Kontakt zum zuständigen Fachbereich**	Gemäß Kundenangaben innerhalb des Hauptvertrages
1.3	**E-Mail-Adresse zur Meldung von Datenschutzvorfällen**	Gemäß Kundenangaben innerhalb des Hauptvertrages

Auftragsverarbeiter:

1.4	**Name und Anschrift**	**Telefónica Germany GmbH & Co. OHG** Georg-Brauchle-Ring 50 80992 München Deutschland
1.5	**Ansprechpartner des Auftragsverarbeiters für Datenschutzfragen** **Kontaktdaten des/der Datenschutzbeauftragten**	Datenschutzbeauftragter Georg-Brauchle-Ring 50 80992 München Deutschland verschlüsseltes Kontaktformular: https://www.telefonica.de/datenschutz-kontakt Mail: datenschutz@telefonica.com

ANHANG II

BESCHREIBUNG DER VERARBEITUNG

2.1.	**Beschreibung der konkreten Datenverarbeitung (Gegenstand, Art und Umfang)**	Telefónica Germany stellt dem Kunden den Mobile Device Management Services („MDM“) zur Verfügung. Dies umfasst die Bereitstellung eines Mobile Device Management Services mit Anbindung an eine MDM-Plattform. Hierfür werden unter anderem die Dienstleister Seven Principles Solutions & Consulting GmbH und Solidas Media eingesetzt. Mittels der MDM-Plattform der Dienstleister werden mobile Geräte (Smartphones oder Tabletts) von Beschäftigten der Endkunden verwaltet. Hierbei nutzt ein registrierter Administrator des Endkunden die Plattformverwaltung für die effiziente Administration der mobilen Endgeräte des Unternehmens (beispielweise zentrale Wartung von Gerätekonfigurationen, Einspielen von Apps etc.) sowie zur Überwachung der Geräte bzgl. Datensicherheit (bspw. Verwaltung des Zugriffs auf Unternehmensdaten durch die mobilen Endgeräte) Um die Verwaltung der Geräte durch die MDM-Plattform zu ermöglichen, werden folgende Daten im System gespeichert: - Gerätedaten des Kunden: Hierbei ist ein Kunde in der Regel eine Firma - Daten des Gerätenutzers (Vorname, Nachname, E-Mailadresse): Gerätenutzer ist in der Regel eine beschäftigte Person des Kunden, kann aber auch beispielsweise ein Fahrzeug sein o.ä. - Administratordaten (Anmeldename und E-Mailadresse): Administrator ist in der Regel eine beschäftigte Person des Kunden oder ein vom Kunden beauftragter Service, welcher von Beschäftigten der Telefónica Germany oder von Telefónica Germany beauftragten Dienstleistern erbracht weren (Verwaltung der Geräte als Managed Service). Die Dienstleister als Betreiber der Plattform haben mit der Rolle des Super-Administrators Zugriff auf die gelisteten personenbezogenen Daten, nehmen aber keine Veränderungen an den personenbezogenen Daten vor, es sei denn auf Anweisung eines weisungsberechtigten Beschäftigten. Die MDM-Plattform wird als Cloud Service dem Kunden durch Telefónica Germany zur Verfügung gestellt. **[Optional]:** Wenn und soweit durch das aktive Hinzubuchen die Funktionserweiterung "o2 Mobile Asset Manager" durch den Auftraggeber genutzt wird, verfügt dieser über die Möglichkeit, die innerhalb der Mobile Device Management Plattform gespeicherten Geräteinformationen über die O_2 Business Easy Access Plattform zu verarbeiten. Hierbei werden die Gerätedaten der Mobile Device Management Plattform in die O_2 Business Easy Access Plattform synchronisiert und mittels API-Schnittstelle verwaltet. Hierdurch erhält der Auftraggeber die Möglichkeit einer vereinfachten Geräte-Konfiguration. das User Interface kann der Bestand der Geräte sowie die Zuordnung der Endgeräte eingesehen werden. Diese Tätigkeiten werden in Systemen, die vom Auftragsverarbeiter (einschließlich seiner Unterauftragsverarbeiter) bereitgestellt werden durchgeführt.

2.2.	**Hauptvertrag (Purchase Order-/ Vertragsbezeichnung):** **Geplante Dauer des Auftrags**	Rahmenvertrag für Produkt (MDM) ☒ befristet bis: Dieser Vertrag ist rechtlich unselbständig und teilt das rechtliche Schicksal des Hauptvertrags. Die Beendigung des Hauptvertrags hat automatisch auch die Beendigung dieser Auftragsverarbeitung zur Folge. Die Parteien sind sich bewusst, dass ohne das Bestehen einer gültigen Datenverarbeitungsvereinbarung keine (weitere) Datenverarbeitung durchgeführt werden darf.
2.3	Bitte hier angeben, welchem **Zweck** die Tätigkeit des Auftragsverarbeiters dient	**1. Zwecke bezüglich Teilnehmende (Kund:innen eines TK-Dienstes) / Nutzende (Nutzende des TK-Dienstes, die selbst nicht Kund:innen sind)** ☒ Begründung (z.B. Bereitstellung Webshop), inhaltliche Ausgestaltung (z.B. Änderungen des Vertrags, Versand von Rechnungen), Beendigung eines Vertragsverhältnisses mit Teilnehmenden, Beratung von Kund:innen (z.B. Kundenservice) ☒ Verwendung für die Bereitstellung von Diensten mit Zusatznutzen (z.B. location based services) ☒ Verwaltung von Teilnehmerdaten (z.B. Betrieb eines CRM-Systems) **2. Zwecke bezüglich Beschäftigten** ☒ Pflege und Verwaltung von Beschäftigtendaten **3. Zwecke bezüglich IT-Leistungen** ☒ Verwaltung von Zugangs-/ Zugriffsrechten auf Informations- und Kommunikationstechnik und Unternehmensnetzwerk ☒ Software-/ Systementwicklung und Testing ☒ Software-/ Systembetrieb ☒ Wartung/ Support (maintenance) **4. Sonstige Zwecke** ☒ *MDM dient der Verwaltung von mobilen Infrastrukturen (Smartphones Tabletts). Zum Zwecke der Fehlererkennung und Entstörung der Geräte werden Gerätedaten verwaltet*
2.4	Bitte hier die **Datenkategorien** angeben, die durch den Auftragsverarbeiter verarbeitet werden	**1. Daten bezüglich Teilnehmende (Kund:innen eines TK-Dienstes) /** Nutzende **(Nutzende des TK-Dienstes, die selbst nicht Kund:innen sind)** ☒ Bestandsdaten nach dem TKG (Vertragliche Angaben, wie Name, Adresse, Bankverbindung, Geburtsdatum, MSISDN, IMEI, IMSI, Kundennummer, Rechnungsnummer, E-Mail-Adresse etc.) ☒ Informationen zu genutzter Hardware oder installierter Software (z.B. Geräte-ID, IMEI, TAC) ☒ Standortdaten (Daten zur Identifizierung eines Standorts eines Endgeräts, Cell-ID, GPS-Daten – *nur soweit diese Funktion aktiv durch den Verantwortlichen aktiviert wurde*) **2. Daten bezüglich Beschäftigten** ☒ Berufliche Kontaktdaten von Beschäftigten, Zeitarbeitenden Praktikant:innen, Auszubildenden (berufliche Telefonnummer/ E-Mail-Adresse, Abteilungszugehörigkeit) ☒ Nutzerkennungen (z.B. Login-Daten, Benutzername und Passwort) **3. Sonstige Datenarten**

		☒ Sonstiges*:* Firmenname, Abteilung/Rolle, Betriebssystem, OS-Version, eID, Apple ID, IMEI, die Kundennummer und die berufliche Mail verarbeitet.
2.5	Die Daten welcher **betroffenen Personen** werden durch den Auftragsverarbeiter verarbeitet?	☒ TK-Dienste-Teilnehmende (Kund:innen eines TK-Dienstes) ☒ TK-Dienste-Nutzende (Nutzende des TK-Dienstes, die selbst nicht Kund:innen ist) ☒ Beschäftigte (z.B. Mitarbeiter:innen, Praktikant:innen, Auszubildende) ☒ Geschäftspartner (z.B. Lieferanten, Distributoren, Vertriebspartner)
2.6	Werden bei den vom Auftragsverarbeiter erbrachten Dienstleistungen **sensible Daten** gemäß Ziffer 7.5 verarbeitet?	☒ Nein
2.7	Bitte geben Sie die **Kategorien der Datenempfänger** an. Übermittelt der Auftragsverarbeiter die Daten im Auftrag des Verantwortlichen an einen Dritten oder einen Auftragsverarbeiter?	☒ Unterauftragsverarbeiter des Auftragsverarbeiters (gilt auch für Konzernunternehmen von Auftragsverarbeitern; Beschreibung der (Unter-) Verarbeitung in **Anhang IV**)
2.8	Bitte geben Sie alle Standorte an, an denen die Daten des Verantwortlichen **gespeichert** sind.	☒ Deutschland
2.9	Bitte geben Sie alle Standorte an, von denen aus auf die Daten des Verantwortlichen wie vorgesehen **zugegriffen** wird.	☒ Deutschland
2.10	Bitte ggf. geltende **gesetzliche Verpflichtungen zur Verarbeitung 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)? ☒ Nein
2.11	Bitte Vorgaben für die **Datenlöschung** machen.	Die Daten des Verantwortlichen (insbesondere Bestands-/ Verkehrs-/ Inhalts- und Beschäftigtendaten) 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 für eine datenschutzgerechte Speicherung von Verkehrsdaten” zu erfolgen.

Es gelten für die vom Auftragsverarbeiter ausgeführte Speicherung der personenbezogenen Daten des Verantwortlichen die folgenden Höchstspeicherfristen:

Wenn eine Löschfrist für Verkehrsdaten nicht bestimmt ist, ist der Auftragsverarbeiter dazu verpflichtet, Verkehrsdaten nach 7 Tagen zu löschen.

Datenart	**Produktivsystem**
Bestandsdaten:	Für die Dauer des aufrechten Vertragsverhältnisses
Verkehrsdaten:	Leitfaden des BfDI für eine datenschutzgerechte Speicherung von Verkehrsdaten
Daten bezüglich Nutzende einer Internetseite, App-Nutzende:	Gemäß Angaben der jeweiligen Datenschutzerklärung
Beschäftigtendaten:	Für die Dauer des aufrechten Vertragsverhältnisses oder früher nach Weisung des Verantwortlichen
Standortdaten/GPS Daten (soweit durch den Kunden aktiviert)	24 Stunden / Archivierung 90 Tage

Nach Beendigung dieses Vertrags sind die Daten des Verantwortlichen binnen folgender Frist zu löschen:

- Digital-Team setzt die Instanz auf "Terminated"
- Die Instanz wird innerhalb 24 Stunden archiviert.
- Das Archiv wir 90 Tage aufbewahrt.

Backups:

	Instanzverzeichnis	Instanzdatenbank
Sicherungsintervall	7 Tage	Täglich
Aufbewahrungsdauer	28 Tage	14 Tage
Mindestanzahl	4 Sicherungen	2 Sicherungen

Archiv:

	Instanzverzeichnis	Instanzdatenbank
Aufbewahrungsdauer	90 Tage	90 Tage
Archivierungsintervall	täglich	täglich

ANHANG III - Technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der personenbezogenen Daten

Ergebnis der Schutzbedarfsanalyse Seven Principles Solutions & Consulting GmbH

Die Vertragspartei hat die datenschutzrechtlichen Risiken für die in ihrem Aufgabenbereich durchgeführte Datenverarbeitung wie folgt definiert:

	Vertraulichkeit	**Integrität**	**Verfügbarkeit**	**Belastbarkeit**
Definition	*Daten dürfen lediglich von autorisierten Benutzern gelesen bzw. modifiziert werden. Dies gilt sowohl beim Zugriff auf gespeicherte Daten wie auch während der Datenübertragung.*	*Daten dürfen nicht unbemerkt oder unautorisiert verändert werden. Alle etwaigen Änderungen müssen nachvollziehbar sein (Daten- & Systemintegrität).*	*Der Zugriff auf die Daten muss innerhalb eines vereinbarten Zeitrahmens gewährleistet werden; Verhinderung von Systemausfällen.*	*Toleranz und Ausgleichsfähigkeit eines Systems gegen Störungen/ Angriffe von innen und außen (Widerstandsfähigkeit, Ausfallsicherheit).*
Sehr hoch	☐	☐	☐	☐
Hoch	☐	☒	☐	☐
Standard	☒	☐	☒	☒

Ergebnis der Schutzbedarfsanalyse Solidas Media GmbH

Die Vertragspartei hat die datenschutzrechtlichen Risiken für die in ihrem Aufgabenbereich durchgeführte Datenverarbeitung wie folgt definiert:

	Vertraulichkeit	**Integrität**	**Verfügbarkeit**	**Belastbarkeit**
Definition	*Daten dürfen lediglich von autorisierten Benutzern gelesen bzw. modifiziert werden. Dies gilt sowohl beim Zugriff auf gespeicherte Daten wie auch während der Datenübertragung.*	*Daten dürfen nicht unbemerkt oder unautorisiert verändert werden. Alle etwaigen Änderungen müssen nachvollziehbar sein (Daten- & Systemintegrität).*	*Der Zugriff auf die Daten muss innerhalb eines vereinbarten Zeitrahmens gewährleistet werden; Verhinderung von Systemausfällen.*	*Toleranz und Ausgleichsfähigkeit eines Systems gegen Störungen/ Angriffe von innen und außen (Widerstandsfähigkeit, Ausfallsicherheit).*
Sehr hoch	☐	☐	☐	☐
Hoch	☐	☒	☐	☐
Standard	☒	☐	☒	☒

		Beschreibung der technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO für den Dienstleister **Seven Principles Solutions & Consulting GmbH**	Beschreibung der technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO für den Dienstleister **Solidas Media GmbH**
3.1	Kommt die von der Telefónica Deutschland zur Verfügung gestellte **VDI** (Virtual Desktop Infrastructure)	☒ Ja	☒ Ja

	Lösung zum Einsatz?		
3.2	Sind **Best Practice Sicherheitsmaßnahmen** (z.B. Sicherheitskonzept nach Art. 32 DS-GVO, internationale Standards) berücksichtigt worden?	☒ Endgerät ist vom Dienstleister verwaltet ☒ Endgerät ist nach dem Stand der Technik geschützt ☒ Sicherheitskonzept (*falls ja, bitte als weitere Anlage diesem Vertrag beifügen*) ☒ Implementierte Sicherheitsmaßnahmen sind immer auf dem Stand der Technik gehalten Zertifizierung/Beachtung internationaler Standards: ☒ Zertifizierung nach ISO 27001	☒ Nein ☒ Endgerät ist nach dem Stand der Technik geschützt Beachtung von internationalen Standards: ☒ Sonstiges (z.B. weitere ISO-Zertifizierung, SOX-Compliance): bitte im Einzelnen aufführen: ISO 9001 2015 Weitere Maßnahmen ☒ Durchgeführte Sicherheitsmaßnahmen sind immer auf dem Stand der Technik gehalten
3.3	Sind Maßnahmen zur **Pseudonymisierung** personenbezogener Daten ergriffen worden?	☒ Nein, weil *(bitte begründen)*: _____ Daten werden auf den Speichermedien verschlüsselt abgelegt (Data at rest encryption), so dass nur über das Frontend von autorisierten Benutzern auf die entschlüsselten Daten zugergriffen werden kann. Dies ist notwendig, da der Verwendungszweck der Plattform sonst nicht erfüllt werden kann. _____	☒ Nein, weil (bitte begründen): Er werden keine personenbezogenen Daten auf Systemen des Auftragnehmer gespeichert, welche über den für den Zweck der Abrechnung benötigten Rahmen hinausgehen.
3.4	Sind Maßnahmen zur räumlichen **Zutrittskontrolle** ergriffen worden, die es Unbefugten verwehren, sich den Systemen, Datenverarbeitungsanlagen oder Verfahren physisch zu nähern, mit denen personenbezogene Daten verarbeitet werden?	☒ Ja Maßnahmen: ☒ Konzept Sicherheitszonen ☒ Schlüsselverwaltung / Dokumentation der Schlüsselvergabe ☒ Zutrittskontrollsystem, z.B. Ausweisleser (Magnet-/Chipkarten) ☒ Werkschutz / Pförtner ☒ Sicherheitstüren / -fenster ☒ Türsicherungen (elektrische Türöffner, Zahlenschloss, etc.) ☒ Alarmanlage ☒ Videoüberwachung ☒ Spezielle Schutzvorkehrungen des Serverraums ☒ Abgeschlossene Aktenschränke ☒ Sonstiges (*bitte aufführen*): _____ Detaillierung im Datensicherheitskonzept_____	☒ Ja Maßnahmen: ☒ Schlüsselverwaltung/ Dokumentation der Schlüsselvergabe ☒ Zutrittskontrollsystem, z.B. Ausweisleser (Magnet-/Chipkarten) ☒ Türsicherungen (elektrische Türöffner, Zahlenschloss, etc.) ☒ Abgeschlossene Aktenschränke ☒ Richtlinie für eine aufgeräumte Arbeitsumgebung ☒ Sonstiges: bitte im Einzelnen aufführen: Zugriff auf Server kann nur durch festgelegte IP Adressen erfolgen, zusätzlich sind diese Verbindungen SSL-verschlüsselt.
3.5	Sind Maßnahmen zur	☒ Ja Maßnahmen:	☒ Ja ☐ Nein, weil *(bitte begründen)*: _____

	Zugangskontrolle ergriffen worden, die gewährleisten, dass ein Zugang durch Unbefugte auf Datenverarbeitungssysteme verhindert wird?	☒ Benutzer haben einen eindeutigen persönlichen Bezeichner ☒ Getrennte Benutzerkennungen für privilegierte Berechtigungen ☒ Benutzerkennungen werden, wenn die Benutzer das Unternehmen verlassen haben, gelöscht oder deaktiviert ☒ Passwörter werden grundsätzlich nicht im Klartext gespeichert oder unverschlüsselt übertragen ☒ Sichere Passwortverfahren ☒ Sichere Erzeugung und Übermittlung von Initial- und Reset-Passwörtern ☒ Automatische Sperrung der Clients nach Zeitablauf ohne Useraktivität (z.B. passwortgeschützter Bildschirmschoner) ☒ Dokumentation administrativer Passwörter in gesicherten Passwortsafes ☒ sichere Verwaltung und Verwendung von digitalem Schlüsselmaterial (z.B.: digitale Zertifikate, Token, etc.) ☒ Regelmäßige Softwareaktualisierung / Patching (Patchmanagement) ☒ Regelmäßige Schwachstellenscans ☒ Netzwerksegmentierung ☒ Firewall, IDS/IPS ☒ Überwachung der Remote-Wartungszugriffe durch Dienstleister ☒ Sonstiges (*bitte aufführen*): _____ Single-Sign-On für die wesentlichen IT-Systeme _____	_____ Maßnahmen: ☒ Benutzer haben einen eindeutigen persönlichen Bezeichner ☒ Getrennte Benutzerkennungen für privilegierte Berechtigungen ☒ Benutzerkennungen werden, wenn die Benutzer das Unternehmen verlassen haben, gelöscht oder deaktiviert ☒ Passwörter werden grundsätzlich nicht im Klartext gespeichert oder unverschlüsselt übertragen ☒ Sichere Passwortverfahren ☒ Sichere Erzeugung und Übermittlung von Initial- und Reset-Passwörtern ☒ Zwei-Faktor-Authentifizierung für kritische Anwendungen ☒ Automatische Sperrung der Clients nach Zeitablauf ohne Useraktivität (z.B. passwortgeschützter Bildschirmschoner) ☒ Dokumentation administrativer Passwörter in gesicherten Passwortsafes ☒ sichere Verwaltung und Verwendung von digitalem Schlüsselmaterial (z.B.: digitale Zertifikate, Token, etc.) ☒ Regelmäßige Softwareaktualisierung / Patching (Patchmanagement) ☒ Regelmäßige Schwachstellenscans ☒ Firewall, IDS/IPS ☒ Sonstiges (*bitte aufführen*): _____ Zugriff auf Server kann nur durch festgelegte IP Adressen erfolgen_____
3.6	Sind Maßnahmen zur **Zugriffskontrolle** ergriffen worden, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass	☒ Ja Maßnahmen: ☒ Inventarisierung der für den Auftrag relevanten Unternehmenswerte ☒ Angemessene Berechtigungskonzepte inkl. der Dokumentation von: ☒ Verantwortlichkeiten ☒ Aufgabenbezogenen Profile und Rollen ☒ Rollenkonzept(e) ☒ Benutzermanagementprozess inkl. Genehmigungsverfahren ☒ Regelmäßige Prüfung der Aktualität von Zugriffsrechten (Rezertifizierung) ☒ Sonstiges (*bitte aufführen*): Detaillierung im Datensicherheitskonzept	☒ Ja Maßnahmen: ☒ Inventarisierung der für den Auftrag relevanten Unternehmenswerte ☒ Angemessene Berechtigungskonzepte inkl. der Dokumentation von: ☒ Verantwortlichkeiten ☒ Aufgabenbezogenen Profile und Rollen

	personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können?		
3.7	Sind Maßnahmen zur **Weitergabekontrolle** 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?	☒ Ja Maßnahmen: ☒ Getunnelte Datenfernverbindungen (VPN = Virtual Private Network) ☒ Gesichertes WLAN ☒ SSL-/TLS-Verschlüsselung ☒ Verschlüsselung von CD/DVD-ROM, externen Festplatten und/oder Laptops ☒ Verwaltung kryptographischer Schlüssel ☒ Richtlinie für eine aufgeräumte Arbeitsumgebung (z.B. Clean-Desk-Policy) ☒ Diebstahlschutz für mobile Geräte ☒ Regelungen zur Datenträgervernichtung, etc. ☒ Sichere, rückstandsfreie Löschung: *Bitte im Einzelnen aufführen*: _____ Lokale Datenhaltung ist im Regelfall nicht vorgesehen. Sollte eine lokale Datenhaltung seitens Telefonica angewiesen werden, dann erfolgt diese auf separater Hardware, welche danach sicher gelöscht wird _____ ☒ Sonstiges (*bitte aufführen*): ___ Detaillierung im Datensicherheitskonzept, keine lokale Datenhaltung regelmäßig zulässig. _____	☒ Ja Maßnahmen: ☒ Verschlüsselung von E-Mail (Ende-zu-Ende) ☒ Getunnelte Datenfernverbindungen (VPN = Virtual Private Network) ☒ Gesichertes WLAN ☒ SSL-/TLS-Verschlüsselung ☒ Verschlüsselung von CD/DVD-ROM, externen Festplatten und/oder Laptops ☒ Diebstahlschutz für mobile Geräte ☒ Regelungen zur Datenträgervernichtung, etc. ☒ Sichere, rückstandsfreie Löschung: *Bitte im Einzelnen aufführen*: BSI IT Baseline Protection
3.8	Sind Maßnahmen zur	☒ Ja	☒ Ja

	Eingabekontrolle 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?	Maßnahmen: ☒ Inventarisierung der für den Auftrag relevanten Daten ☒ Berechtigungskonzepte vorhanden, inkl. der Dokumentation von: ☒ Funktionalen Verantwortlichkeiten ☒ Need-to-know Prinzip (allgemein) ☒ Angemessener Funktionstrennung ☒ Sonstiges (*bitte aufführen*): Detaillierung im Datensicherheitskonzept _____	Maßnahmen: ☒ Berechtigungskonzepte vorhanden, inkl. der Dokumentation von: ☒ Funktionalen Verantwortlichkeiten ☒ Need-to-know Prinzip (allgemein) ☒ Angemessener Funktionstrennung
3.9	Sind Maßnahmen zur **Auftragskontrolle** ergriffen worden, die sicherstellen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden können?	☒ Ja Maßnahmen: ☒ Verbindliche Sicherheitsleitlinien inkl. Verpflichtungen der Mitarbeiter ☒ Schulungen aller zugriffsberechtigten Mitarbeiter ☒ Regelmäßig stattfindende Nachschulungen ☒ Betriebshandbücher für den sicheren Betrieb ☒ Regelmäßige Datenschutzaudits des betrieblichen Datenschutzbeauftragten ☒ Prüfungsplanung für interne und externe Audits ☒ Nutzung eines risikoorientierten Auditansatzes ☒ Monitoring & Reporting über neu identifizierte Risiken / Schwachstellen ☒ IT-Change Management Prozess ☒ Trennung von Entwicklungs- und Produktivsystemen inkl. geregeltem Transportprozess (production take over) ☒ Durchführung von Funktions- und Benutzerakzeptanztests ☒ Genehmigungs- und Freigabeverfahren ☒ Regeln für die sichere Entwicklung von Software und Systemen sind festgelegt und werden angewandt ☒ Zugriff auf Source-Code / Customizing geschützt (need-to-know-Prinzip) ☒ Sonstiges (*bitte aufführen*): ITIL konformer Mangementprozess _____	☒ Ja Maßnahmen: ☒ Verbindliche Sicherheitsleitlinien inkl. Verpflichtungen der Mitarbeiter ☒ Schulungen aller zugriffsberechtigten Mitarbeiter ☒ Regelmäßig stattfindende Nachschulungen ☒ Regelmäßige Datenschutzaudits des betrieblichen Datenschutzbeauftragten ☒ Prüfungsplanung für interne und externe Audits ☒ Nutzung eines risikoorientierten Auditansatzes ☒ Monitoring & Reporting über neu identifizierte Risiken / Schwachstellen ☒ IT-Change Management Prozess

3.10	Sind Maßnahmen zur **Verfügbarkeitskontrolle** ergriffen worden, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind bzw. zügig wiederhergestellt werden können?	☒ Ja Maßnahmen: ☒ Service Level Agreements (SLAs) mit Dienstleistern ☒ Backup Verfahren ☒ Sichere Aufbewahrung für Backups (z.B. Safe, getrennter Brandabschnitt) ☒ Viren-/Schadcodeschutz ☒ Redundante Komponenten (z.B. Spiegeln von Festplatten) ☒ Redundante Versorgung (z.B. Internet, Telefon, Strom) ☒ Geeignete Archivierungsräumlichkeiten ☒ Schutz der relevanten Infrastruktur gegen Defekte durch äußere Einflüsse ☒ Pläne für Ausfall / Notfall / Wiederanlauf etc. (einzelner Komponenten) ☒ Sonstiges (*bitte aufführen*): ___ Detaillierung im Datensicherheitskonzept _____	☒ Ja Maßnahmen: ☒ Sichere Aufbewahrung für Backups (z.B. Safe, getrennter Brandabschnitt) ☒ Redundante Komponenten (z.B. Spiegeln von Festplatten) ☒ Redundante Komponenten (z.B. Spiegeln von Festplatten) ☒ Redundante Versorgung (z.B. Internet, Telefon, Strom): redundante VoIP TK , redundante Internetverbindung ☒ Schutz der relevanten Infrastruktur gegen Defekte durch äußere Einflüsse ☒ Pläne für Ausfall / Notfall / Wiederanlauf etc. (einzelner Komponenten)
3.11	Sind Maßnahmen zur Einhaltung des **Trennungsgebots** ergriffen worden, die gewährleisten, dass Daten, die zu unterschiedlichen Zwecken erhoben werden, getrennt verarbeitet (z.B. gelöscht) werden können.	☒ Ja Maßnahmen: ☒ Getrennte Datenbanken ☒ Trennung durch Zugriffsregelungen	☒ Nein, weil *(Bitte begründen)*: Es werden nur diese Daten gespeichert, welche für Abrechnungszwecke benötigt werden. Insofern ist keine Trennung erforderlich.
3.12	Sind Maßnahmen und Verantwortlichkeiten für den **Umgang mit Informations-sicherheitsvorfällen und Krisensituationen** definiert worden?	☒ Ja Maßnahmen: ☒ Managementprozess für Security Incidents ☒ Managementprozess für datenschutzrelevante Incidents ☒ Definition der Sicherheitsanforderungen in Krisensituation / im Notfall ☒ Übergreifender Notfallplan inkl. regelmäßiger Aktualisierung	☒ Ja Maßnahmen: ☒ Managementprozess für Security Incidents ☒ Managementprozess für datenschutzrelevante Incidents ☒ Übergreifender Notfallplan inkl. regelmäßiger Aktualisierung

			☒ Regelmäßige Durchführung und Dokumentation von Notfalltests / Notfallübungen
3.13	Sind Maßnahmen für **Logging** in den relevanten Bereichen ergriffen worden?	☒ Ja ☒ Die Log-Systeme beziehen sich auf eine einzige Zeitquelle ☒ Verarbeitung der Daten in Übereinstimmung mit geltenden gesetzlichen Bestimmungen für die Informationssicherheit ☒ Logs sind gegen unberechtigten Zugriff geschützt (Vertraulichkeit) ☒ Logs sind vor unberechtigter Veränderung geschützt (Integrität) ☒ Logs sind vor Verlust geschützt (Verfügbarkeit) **Eingabekontrolle** ☒ Systemseitiges Logging von Eingaben **Verfügbarkeitskontrolle** ☒ Logging der Verfügbarkeit ☒ Regelmäßige Überwachung der Systeme und Logfiles **Zutrittskontrolle** ☒ Logging der Zutritte ☒ Regelmäßiges Monitoring von Zutritten ☒ Auswertung der Logs zur weiteren Verwendung **Zugangskontrolle** ☒ Logging der Zugänge ☒ Personenbezogenes Logging: *bitte spezifizieren, welche für den Auftrag relevanten Daten geloggt werden:*__ Es erfolgt eine Authentifizierung des Zugriffs über die persönliche Authentifizierung über Zugriffsschlüssel_____ ☒ Auswertung der Logs zur weiteren Verwendung **Zugriffskontrolle** ☒ Logging der Zugriffe ☒ schreibend ☒ Regelmäßiges Monitoring von Zugriffen: *bitte spezifizieren, welche Parameter regelmäßig überwacht werden:*__ Das Logging wird von dem Anwendungssystem zur Verfügung gestellt und die Nutzung ist in Kundenhoheit. Operative Zugriffe auf das Betriebssystem werden über das System Logging protokolliert_____	☒ Ja ☒ Logs sind gegen unberechtigten Zugriff geschützt (Vertraulichkeit) ☒ Logs sind vor unberechtigter Veränderung geschützt (Integrität) ☒ Logs sind vor Verlust geschützt (Verfügbarkeit)

3.14	Ist Mitarbeitern erlaubt aus dem **Home Office** zu arbeiten? Sind Maßnahmen zur Arbeit im Homeoffice bzw. für Telearbeit ergriffen worden? *Beachte: Die Verarbeitung von personenbezogenen Daten des Verantwortlichen außerhalb der Betriebsstätte des Auftragsverarbeiters (z.B. im Homeoffice oder bei sonstigem Remote-Zugriff) ist nur zulässig, sofern geeignete Maßnahmen nach Art. 32 DSGVO ergriffen sind und keine Verkehrsdaten, Inhaltsdaten und keine besonderen Kategorien von personenbezogenen Daten verarbeitet werden (vgl. Annex V Ziffer 2).*	☒ Ja ☒ Home Office Richtlinie / besondere Arbeitsanweisungen ☒ Untersagung mobiles Arbeiten in öffentlichen Bereichen ☒ Verschlüsselung der Remoteverbindung als Arbeitsumgebung ☒ Organisatorische und physische Maßnahmen zur Gewährleistung der Vertraulichkeit	☒ Ja ☒ Home Office Richtlinie / besondere Arbeitsanweisungen ☒ Untersagung mobiles Arbeiten in öffentlichen Bereichen ☒ Verschlüsselung der Remoteverbindung

ANHANG IV – LISTE DER UNTERAUFTRAGSVERARBEITER

Angabe des Unterauftragsverarbeiters	Beschreibung der Verarbeitung	Bestehen Verträge zur Unter-Auftragsverarbeitung (Art. 28 Abs. 4 DSGVO)?	Findet eine Übermittlung von oder ein Zugriff auf die Daten des Verantwortlichen in/aus Drittländern (außerhalb der EU/des EWR) statt?
Name/ Firma: Telefónica Cybersecurity & Cloud Tech Deutschland GmbH **Anschrift:** Adalperostraße 82-86 85737 Ismaning Deutschland	Betrieb der MDM-Plattform **Ort der Datenspeicherung:** (1) Seven Principles Solutions & Consulting GmbH Rechenzentrum Frankfurt (2) SOLIDAS Media GmbH Plönzeile 17 12459 Berlin	☒ Ja, Vereinbarungen gemäß Art. 28 Abs. 4 DSGVO bestehen	☒ Nein, eine Zugriffsmöglichkeit auf diese Daten von außerhalb der EU/des EWR ist technisch ausgeschlossen.

ANHANG V ERGÄNZENDE REGELUNGEN ZUM AVV

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.

1. Vertraulichkeit und Geheimhaltung der Telekommunikation

1.1 Der Auftragsverarbeiter kennt und beachtet die Datenschutzregeln nach §§ 1 ff. Telekommunikations- und Telemedien-Datenschutzgesetz (TTDSG), soweit diese nach der Verordnung (EU) 2016/679 (DSGVO) weiterhin gelten, sowie das Fernmeldegeheimnis gemäß § 3 TTDSG.

1.2 Ergänzend zu Ziffer 7.4 b der AVV stellt der Auftragsverarbeiter sicher, dass sich die zur Verarbeitung von Verkehrsdaten und Inhaltsdaten (ANHANG II, 2.4) im Auftrag des Verantwortlichen befugten Personen zum Fernmeldegeheimnis gemäß § 3 TTDSG verpflichtet haben. Das Fernmeldegeheimnis bleibt auch nach Beendigung der AVV bestehen.

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. Der Auftragsverarbeiter legt dem Verantwortlichen eine Dokumentation der implementierten technischen und organisatorischen Maßnahmen für derartige Remote-Zugriffe vor (siehe ANHANG III, 3.14).

3. Dokumentation und Einhaltung der Klauseln

3.1 Zusätzlich zu Klausel 7.1 (a) wird der Verantwortliche mündliche Weisungen unverzüglich in Textform bestätigen.

3.2 Eine Kündigung nach der Klausel 10 (c) setzt ergänzend zu den dort geregelten Voraussetzungen weiter voraus, dass dem Verantwortlichen unter Berücksichtigung aller Umstände des Einzelfalls und unter Abwägung der beiderseitigen Interessen die Fortsetzung des Vertragsverhältnisses bis zur vereinbarten Beendigung oder bis zum Ablauf einer Kündigungsfrist nicht zugemutet werden kann. Etwaige Rechte der Parteien zur außerordentlichen Kündigung nach dem anwendbaren Recht bleiben hiervon unberührt.

4. Haftung

Etwaige Haftungsbeschränkungen aus einem ggf. geschlossenen Hauptvertrag oder den übrigen Anhängen zu dem Hauptvertrag finden auf diesen Vertrag Anwendung.

5. Sonstige Bestimmungen

5.1 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.

5.2 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.

5.3 Soweit rechtlich zulässig und in einem ggf. geschlossenen Hauptvertrag nichts Abweichendes bestimmt ist, gilt deutsches Recht und der Gerichtsstand München.