# Annex Auftragsverarbeitungsvertrag

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 „**$O_2$ Business Device-as-a-Service - DaaS"** Leistungen („**Hauptvertrag**") ergeben. Der Annex findet Anwendung auf alle Tätigkeiten, bei denen der Auftragnehmer personenbezogene Daten des Auftraggebers („**Auftraggeber-Daten**") verarbeitet. 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 Device-as-a-Service - DaaS** 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 Hauptvertrags durch die Parteien zustande. Der Kunde ist für die Datenverarbeitung im Zusammenhang mit **$O_2$ Business Device-as-a-Service - DaaS** 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 Digitale Dienste-Recht 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 Hauptvertrags |
| 1.2 | **Kontakt zum zuständigen Fachbereich** | Gemäß Kundenangaben innerhalb des Hauptvertrags |
| 1.3 | **E-Mail-Adresse zur Meldung von Datenschutzvorfällen** | Gemäß Kundenangaben innerhalb des Hauptvertrags |

### Auftragsverarbeiter:

| | | |
|---|---|---|
| 1.4 | **Name und Anschrift** | **Telefónica Germany GmbH & Co. OHG**<br>Georg-Brauchle-Ring 50<br>80339 München |
| 1.5 | **Ansprechpartner des Auftragsverarbeiters für Datenschutzfragen** | **Telefónica Germany GmbH & Co. OHG**<br>z. Hd. Datenschutzbeauftragter<br>Mail: datenschutz@telefonica.com<br>Georg-Brauchle-Ring 50<br>80992 München<br>verschlüsseltes Kontaktformular:<br>https://www.telefonica.de/datenschutz-kontakt |

## ANHANG II - BESCHREIBUNG DER VERARBEITUNG

| | | |
|---|---|---|
| 2.1. | **Beschreibung der konkreten Datenverarbeitung (Gegenstand, Art und Umfang)** | Der Auftragsverarbeiter betreibt das unter dem Namen $O_2$ Business Device-as-a-Service (DaaS) bekannte Produkt zur Verfügung. Details zum Gegenstand der Verarbeitung ergeben sich jeweils aus dem zwischen den Parteien geschlossenen, diesem Vertrag zugrunde liegenden Hauptvertrag und seinen Anlagen, insbesondere der Leistungsbeschreibung der Telefónica Germany GmbH & Co. OHG für Hardwaremiete – $O_2$ Business Device-as-a-Service. Gegenstand der Auftragsverarbeitung ist die Bereitstellung, Konfiguration, Verwaltung, Entstörung sowie Rückführung und Datenlöschung mobiler Endgeräte im Rahmen des Device-as-a-Service-Dienstes.<br>Diese Tätigkeiten werden in Systemen, die vom Auftragsverarbeiter (inkl. dessen Unterauftragsverarbeitern) bereitgestellt werden, durchgeführt. 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. |
| 2.2. | **Hauptvertrag (Vertragsbezeichnung):**<br><br>**Geplante Dauer des Auftrags** | Vertrag $O_2$ Business Device-as-a-Service<br><br>☒ befristet bis: Vorliegender Auftragsverarbeitungsvertrag ist rechtlich unselbständig und teilt das rechtliche Schicksal des Hauptvertrags; eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses Vertrags. Es ist den Parteien bewusst, dass ohne Vorliegen eines gültigen Auftragsverarbeitungsvertrags keine (weitere) Auftragsverarbeitung durchgeführt werden darf. Eine isolierte ordentliche Kündigung dieses Vertrags ist ausgeschlossen. |
| 2.3 | Die Daten welcher **betroffenen Personen** werden durch den Auftragsverarbeiter verarbeitet? | ☒ Gerätenutzer / „End User“<br>☒ Ansprechpartner, Beschäftigte und sonstige vom Auftraggeber autorisierte natürliche Personen des Geschäftskunden von Telefónica Germany |
| 2.4 | Bitte hier angeben, welchem **Zweck** die Tätigkeit des Auftrags-verarbeiters dient | **1. Zwecke bezüglich Gerätebereitstellung und Staging**<br>☒ Individuelle Konfiguration und Initialisierung der Endgeräte, einschließlich der Einrichtung des Device Enrollment,<br>☒ Ausführung initialer Softwareupdates, der physischen Einlage von SIM-Karten bzw. der Aktivierung von eSIM-Profilen<br>☒ Geräteindividuelle Vorbereitung für den Einsatz im betrieblichen Umfeld des Auftraggebers<br><br>**2. Zwecke bezüglich Nutzerverwaltung und Geräteflottenbetrieb**<br>☒ Geräte-Nutzer-Zuordnung, Anlage und Verwaltung von Nutzerprofilen, sowie Administration der Geräteflotte des Auftraggebers<br><br>**3. Zwecke bezüglich Rückgabeabwicklung**<br>☒ Steuerung und Koordination des Rückgabeprozesses bei Ablauf der vereinbarten Mietdauer, einschließlich der Zusendung individueller |

| | | |
|---|---|---|
| | | Rücksendelabels an die designierten Gerätenutzer und der Übergangskoordination zum Anschlussgerät<br>☒ Durchführung der zertifizierten Löschung sämtlicher auf den zurückgegebenen Endgeräten lokal gespeicherter personenbezogener Daten gemäß den Weisungen des Auftraggebers sowie anerkannter technischer Standards mit anschließender Löschbestätigung |
| 2.5 | Bitte hier die **Datenkategorien** angeben, die durch den Auftragsverarbeiter verarbeitet werden | **1. Identifikations- und Kontaktdaten der Gerätenutzer**<br>☒ Bestandsdaten nach dem TKG (vertragliche Angaben wie Name, Adresse, Bankverbindung, Geburtsdatum, MSISDN, IMSI, Kundennummer, E-Mail-Adresse, Packs und Optionen)<br>☒ Vor- und Nachname<br>☒ Geschäftliche E-Mail-Adresse<br>☒Telefonnummer (soweit für die Abwicklung des Austausch- oder Rückgabeprozesses erforderlich)<br>☒ Informationen zu genutzter Hardware oder installierter Software (z.B. Geräte-ID, IMEI, TAC)<br><br>**2. Geräte- und vertragsbezogene Daten mit Personenbezug**<br>☒ Gerätekennung (IMEI, Seriennummer des Endgeräts)<br>☒ SIM-Kartennummer (ICCID) bzw. eSIM-Profil-Identifikation<br>☒ Mobilfunknummer (MSISDN)<br>☒ Geräte-Nutzer-Zuordnung (Verknüpfung von IMEI / Seriennummer mit dem jeweiligen Nutzerprofil – soweit vorhanden)<br>☒ Nutzerbezogene Bestell- und Nachbestellhistorie<br><br>**3. Daten bezüglich Kunden**<br>☒ Kundenbestandsdaten (vertragliche Angaben, wie Name, Adresse, Bankverbindung, Geburtsdatum, Kundennummer, E-Mail-Adresse)<br>☒ Rechnungen<br>☒ Beschäftigtenstammdaten<br><br>**4. Verwaltungs- und Zugriffsdaten**<br>☒ Anmeldedaten und Nutzerprofile der Administratoren (Benutzername, Anmeldeinformationen, Zugriffsrollen)<br>☒ Aktivitätsprotokolle (Audit-Logs) für administrative Verwaltungshandlungen mit Personenbezug<br>☒ Berufliche Kontaktdaten von Beschäftigten, Zeitarbeitenden Praktikanten, Auszubildenden (berufliche Telefonnummer/ E-Mail-Adresse, Abteilungszugehörigkeit)<br><br>**5. Auf zurückgegebenen Endgeräten gespeicherte personenbezogene Daten**<br>☒ Sämtliche zum Zeitpunkt der physischen Rückgabe auf dem jeweiligen Endgerät lokal gespeicherten personenbezogenen Daten (Art, Umfang und Inhalt dieser Daten liegen im alleinigen Verantwortungsbereich des Auftraggebers und sind dem Auftragnehmer inhaltlich nicht zur Kenntnis zu bringen; die Verarbeitung beschränkt sich ausschließlich auf den technischen Löschvorgang.) |
| 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<br>☐ EU/EWR abgesehen von Deutschland<br>☐ Drittländer wie folgt (außerhalb des EU/EWR-Raums)<br>*Bitte konkret angeben:* |
| 2.9 | Bitte geben Sie alle Standorte an, von denen aus auf die Daten des Verantwortlichen wie vorgesehen **zugegriffen** wird. | ☒ Deutschland<br>☐ EU/EWR abgesehen von Deutschland<br>☐ Drittländer wie folgt (außerhalb des EU/EWR-Raums)<br>*Bitte konkret angeben:* |
| 2.11 | Bitte Vorgaben für die **Datenlöschung** machen. | Die Daten des Verantwortlichen 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 Erforderlichkeit der Datenspeicherung bemisst sich nach dem Zweck, zu dem sie erfasst wurden. Das bedeutet, dass personenbezogene Daten in Systemen vernichtet oder gelöscht werden müssen, wenn sie nicht länger benötigt werden. Maßgeblich hierfür ist, dass personenbezogene Daten entsprechend der folgenden Logik verarbeitet und aufbewahrt werden:<br><br>i. solange die Daten verwendet werden, um einen der hier genannten Dienste bereitzustellen,<br>ii. wie laut geltendem Recht, Vertrag oder im Hinblick auf unsere gesetzlichen Verpflichtungen erforderlich oder<br>iii. so lange, wie dies zur Erreichung der vorstehend geschilderten Zwecke erforderlich ist, oder länger, wenn dies vertraglich, gesetzlich oder zu statistischen oder Beweiszwecken erforderlich ist, unter Anwendung angemessener Schutzmaßnahmen.<br><br>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. Sicherheitskopien von Bestandsdaten und Admin User Logs werden – soweit notwendig - für maximal ein Jahr aufbewahrt (Höchstspeicherfrist). Der Auftragsverarbeiter vernichtet diese Datensätze ohne Aufforderung des Verantwortlichen mit Ablauf der Aufbewahrungspflichten bzw. mit Wegfall der Notwendigkeit der Datenspeicherung zu Sicherheitszwecken. Es wird keine Archivierung für den Verantwortlichen durch den Auftragnehmer durchgeführt. |

## ANHANG III – TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER PERSONENBEZOGENEN DATEN

| | | |
|---|---|---|
| 3.1 | Sind **Best Practice Sicherheitsmaßnahmen** (z.B. Sicherheitskonzept nach Art. 32 DS-GVO, internationale Standards) berücksichtigt worden? | ☒ Endgerät ist vom Dienstleister verwaltet<br>☒ Endgerät ist nach dem Stand der Technik geschützt<br>☒ Sicherheitskonzept<br>☒ Dokumentation der technischen und organisatorischen Maßnahmen<br>☒ Implementierte Sicherheitsmaßnahmen sind immer auf dem Stand der Technik gehalten<br>☒ Datenschutzrichtlinie<br>☒ Zertifizierung nach ISO 27001 |
| 3.2 | Sind Maßnahmen zur **Pseudonymisierung** personenbezogener Daten ergriffen worden? | ☒ Ja: Eine Pseudonymisierung erfolgt auf Basis einer Useranordnung anhand von IMEI und/oder UserID, die nicht auf eine natürliche Person schließen lässt - lediglich für den Versand sind Klarnamen und Adressen ersichtlich. Diese wurden dann in jedem einzelnen Fall vom User selbst freigegeben zur Verarbeitung und sind bis zum Versand in den Systemen gespeichert. Bei einem erneuten Versand muss der User und/oder der Kunde aktiv Namen und Adresse erneut angeben. |
| 3.3 | 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<br><br>Maßnahmen:<br>☒ Schlüsselverwaltung / Dokumentation der Schlüsselvergabe<br>☒ Zutrittskontrollsystem, z.B. Ausweisleser (Magnet-/Chipkarten)<br>☒ Alarmanlage<br>☒ Videoüberwachung<br>☒ Abgeschlossene Aktenschränke |
| 3.4 | Sind Maßnahmen zur **Zugangskontrolle** ergriffen worden, die gewährleisten, dass ein Zugang durch Unbefugte auf Datenverarbeitungssysteme verhindert wird? | ☒ Ja<br><br>Maßnahmen:<br>☒ Benutzer haben einen eindeutigen persönlichen Bezeichner<br>☒ Getrennte Benutzerkennungen für privilegierte Berechtigungen<br>☒ Benutzerkennungen werden, wenn die Benutzer das Unternehmen verlassen haben, gelöscht oder deaktiviert<br>☒ Passwörter werden grundsätzlich nicht im Klartext gespeichert oder unverschlüsselt übertragen<br>☒ Sichere Passwortverfahren<br>☒ Sichere Erzeugung und Übermittlung von Initial- und Reset-Passwörtern<br>☒ Zwei-Faktor-Authentifizierung für kritische Anwendungen<br>☒ Automatische Sperrung der Clients nach Zeitablauf ohne Useraktivität (z.B. passwortgeschützter Bildschirmschoner)<br>☒ Dokumentation administrativer Passwörter in gesicherten Passwortsafes<br>☒ sichere Verwaltung und Verwendung von digitalem Schlüsselmaterial (z.B.: digitale Zertifikate, Token, etc.)<br>☒ Regelmäßige Softwareaktualisierung / Patching (Patchmanagement)<br>☒ Regelmäßige Schwachstellenscans<br>☒ Firewall, IDS/IPS<br>☒ Überwachung der Remote-Wartungszugriffe durch Dienstleister |

| | | |
|---|---|---|
| 3.5 | 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 personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können? | ☒ Ja<br><br>Maßnahmen:<br>☒ Angemessene Berechtigungskonzepte inkl. der Dokumentation von:<br>☒ Verantwortlichkeiten<br>☒ Aufgabenbezogenen Profile und Rollen<br>☒ Rollenkonzept(e) |
| 3.6 | 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<br><br>Maßnahmen:<br>☒ Gesichertes WLAN<br>☒ SSL-/TLS-Verschlüsselung<br>☒ Verschlüsselung von CD/DVD-ROM, externen Festplatten und/oder Laptops<br>☒ Elektronische Signatur<br>☒ Verwaltung kryptographischer Schlüssel<br>☒ Richtlinie für eine aufgeräumte Arbeitsumgebung (z.B. Clean-Desk-Policy)<br>☒ Diebstahlschutz für mobile Geräte<br>☒ Regelungen zur Datenträgervernichtung, etc.<br>☒ Sichere, rückstandsfreie Löschung: Löschung mobiler Endgeräte mit BSI zertifizierter Blancco Software |
| 3.7 | Sind Maßnahmen zur **Eingabekontrolle** ergriffen worden, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungs-systeme eingegeben, verändert oder entfernt worden sind? | ☒ Ja<br><br>Maßnahmen:<br>☒ Inventarisierung der für den Auftrag relevanten Daten<br>☒ Berechtigungskonzepte vorhanden, inkl. der Dokumentation von:<br>☒ Need-to-know Prinzip (allgemein)<br>☒ Angemessener Funktionstrennung |
| 3.8 | Sind Maßnahmen zur **Auftragskontrolle** ergriffen worden, die sicherstellen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen | ☒ Ja<br><br>Maßnahmen:<br>☒ Verbindliche Sicherheitsleitlinien inkl. Verpflichtungen der Mitarbeiter<br>☒ Schulungen aller zugriffsberechtigten Mitarbeiter<br>☒ Regelmäßig stattfindende Nachschulungen<br>☒ Betriebshandbücher für den sicheren Betrieb<br>☒ Regelmäßige Datenschutzaudits des betrieblichen Datenschutzbeauftragten |

| | | |
|---|---|---|
| | verarbeitet werden können? | ☒ Prüfungsplanung für interne und externe Audits<br>☒ Nutzung eines risikoorientierten Auditansatzes<br>☒ Monitoring & Reporting über neu identifizierte Risiken / Schwachstellen<br>☒ Verbot der Installation nicht freigegebener Software / Applikationen auf den Endgeräten<br>☒ Trennung von Entwicklungs- und Produktivsystemen inkl. geregeltem Transportprozess (production take over)<br>☒ Durchführung von Funktions- und Benutzerakzeptanztests<br>☒ Genehmigungs- und Freigabeverfahren<br>☒ Regeln für die sichere Entwicklung von Software und Systemen sind festgelegt und werden angewandt<br>☒ Zugriff auf Source-Code / Customizing geschützt (need-to-know-Prinzip) |
| 3.9 | Sind Maßnahmen zur **Verfügbarkeitskontrolle** ergriffen worden, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind bzw. zügig wiederhergestellt werden können? | ☒ Ja<br><br>Maßnahmen:<br>☒ Business Continuity Strategie und Management<br>☒ Service Level Agreements (SLAs) mit Dienstleistern<br>☒ Backup Verfahren<br>☒ Sichere Aufbewahrung für Backups (z.B. Safe, getrennter Brandabschnitt)<br>☒ Viren-/Schadcodeschutz<br>☒ Redundante Komponenten (z.B. Spiegeln von Festplatten)<br>☒ Redundante Versorgung (z.B. Internet, Telefon, Strom)<br>☒ Pläne für Ausfall / Notfall / Wiederanlauf etc. (einzelner Komponenten) |
| 3.10 | 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<br><br>Maßnahmen:<br>☒ Getrennte Systeme<br>☒ Getrennte Datenbanken<br>☒ Trennung durch Zugriffsregelungen |
| 3.11 | Sind Maßnahmen und Verantwortlichkeiten für den **Umgang mit Informations-sicherheitsvorfällen und Krisensituationen** definiert worden? | ☒ Ja<br><br>Maßnahmen:<br>☒ Managementprozess für Security Incidents<br>☒ Managementprozess für datenschutzrelevante Incidents<br>☒ Definition der Sicherheitsanforderungen in Krisensituation / im Notfall |
| 3.12 | Sind Maßnahmen für **Logging** in den relevanten Bereichen ergriffen worden? | ☒ Ja<br><br>☒ Es existiert ein dokumentiertes Loggingkonzept<br>☒ Verarbeitung der Daten in Übereinstimmung mit geltenden gesetzlichen Bestimmungen für die Informationssicherheit<br>☒ Logs sind gegen unberechtigten Zugriff geschützt (Vertraulichkeit)<br>☒ Logs sind vor unberechtigter Veränderung geschützt (Integrität)<br>☒ Logs sind vor Verlust geschützt (Verfügbarkeit)<br><br>**Eingabekontrolle**<br>☒ Systemseitiges Logging von Eingaben |

| | | |
|---|---|---|
| | | **Verfügbarkeitskontrolle**<br>☒ Logging der Verfügbarkeit<br>☒ Regelmäßige Überwachung der Systeme und Logfiles<br><br>**Zutrittskontrolle**<br>☒ Logging der Zutritte<br><br>**Zugangskontrolle**<br>☒ Logging der Zugänge<br>☒ Regelmäßiges Monitoring von VPN-Anmeldungen inkl. Geo-IP<br><br>**Zugriffskontrolle**<br>☒ Logging der Zugriffe<br>☒ schreibend<br>☒ Auswertung der Logs zur weiteren Verwendung |
| 3.13 | Ist Mitarbeitern erlaubt aus dem **Home Office** zu arbeiten? Sind Maßnahmen zur Arbeit im Homeoffice bzw. für Telearbeit ergriffen worden? | ☒ Ja<br><br>Maßnahmen:<br>☒ Home Office Richtlinie / besondere Arbeitsanweisungen<br>☒ Vorgaben zur heimischen Infrastruktur<br>☒ Verbot von Aufzeichnungen (digital oder in Papierform)<br>☒ Pflicht zum Einsatz von USB-Headsets (keine Möglichkeit zur Freisprechung)<br>☒ Verbot von Bluetooth-Devices (z.B. Maus, Headset, Tastatur)<br>☒ Sanktionen bei Verstößen<br>☒ Untersagung mobiles Arbeiten in öffentlichen Bereichen<br>☒ Verbot der Privatnutzung geschäftlicher Ausstattung<br>☒ Regelmäßige Bestätigung der Einhaltung der Home Office Richtlinie<br>☒ Zwei-Faktor-Authentifizierung<br>☒ VPN mit Zwei-Faktor-Authentifizierung, ohne Split Tunneling<br>☒ Virtuelle Desktops, Jump Server im Unternehmen<br>☒ Organisatorische und physische Maßnahmen zur Gewährleistung der Vertraulichkeit<br>☒ Schutz vor Datenweitergabe vom Endgerät |

## ANHANG IV – LISTE DER UNTERAUFTRAGSVERARBEITER

ERLÄUTERUNG: Dieser Anhang muss im Falle einer gesonderten Genehmigung von Unterauftragsverarbeitern ausgefüllt werden (Klausel 7.7 Buchstabe a).

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

| **Lfd. Nr.** | **Angabe des Unterauftragsverarbeiters** | **Beschreibung der Verarbeitung** | **Bestehen Verträge zur Unter-Auftragsverarbeitung (Art. 28 Abs. 4 DSGVO)?** **Die zwischen den Auftragsverarbeitern abgeschlossenen Datenschutzvereinbarungen inklusive Nachweisen zu technischen und organisatorischen Maßnahmen sind vor dem Abschluss dieses Vertrags auf Anforderung vorzulegen.** | **Findet eine Übermittlung von oder ein Zugriff auf die Daten des Verantwortlichen in/aus Drittländern (außerhalb der EU/des EWR) statt?** | **Hat der Auftragsverarbeiter gesetzlich vorgeschriebene Garantien, ein Transfer Impact Assessment (TIA) und, soweit relevant, Supplementary Measures (vgl. EDPB, Empfehlungen 01/2020) gemäß Kapitel V der DSGVO implementiert?** |
|---|---|---|---|---|---|
| **1.** | **Name/Firma:**<br>greendevice business GmbH<br><br>**Adresse:**<br>Butzweilerhofallee 2<br>50829 Köln<br><br>**Ort der Speicherung/ des bestimmungsgemäßen Zugriffs auf die im Auftrag verarbeiteten Daten**<br>Deutschland | Durchführung der Löschung und Unterstützung des Auftragsverarbeiters in der Erbringung der Leistungen<br><br>**Beauftragt von:**<br>☒ Auftragsverarbeiter | ☒ Ja, Vereinbarungen gemäß Art. 28 Abs. 4 DSGVO bestehen | ☒ Nein, eine Zugriffsmöglichkeit auf diese Daten von außerhalb der EU/des EWR ist technisch ausgeschlossen. | ☒ n/a |
| **2.** | **Name/Firma:**<br>Telefonica Germany Customer Service Nürnberg GmbH<br><br>**Adresse:**<br>Südwestpark 37-41<br>90449 Nürnberg<br><br>**Ort der Speicherung/ des bestimmungsgemäßen Zugriffs auf die im Auftrag verarbeiteten Daten**<br>Deutschland | Manuelle Ein- und Ausbuchung (Enrollment/De-Enrollment) von SIM-Karten und Endgeräten – inkl. Einschreibung, Anmeldung bzw. Registrierung sowie deren Rückgängigmachung und Deaktivierung<br><br>**Beauftragt von:**<br>☒ Auftragsverarbeiter | ☒ Ja, Vereinbarungen gemäß Art. 28 Abs. 4 DSGVO bestehen | ☒ Nein, eine Zugriffsmöglichkeit auf diese Daten von außerhalb der EU/des EWR ist technisch ausgeschlossen. | ☒ n/a |

## 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 Digitale Dienste-Recht zu entsprechen.

### 1. Vertraulichkeit und Geheimhaltung der Telekommunikation

1.1 Der Auftragsverarbeiter kennt und beachtet die Datenschutzregeln nach §§ 1 ff. Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG), soweit diese nach der Verordnung (EU) 2016/679 (DSGVO) weiterhin gelten, sowie das Fernmeldegeheimnis gemäß § 3 TDDDG.

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, 2.5) im Auftrag des Verantwortlichen befugten Personen zum Fernmeldegeheimnis gemäß § 3 TDDDG 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) der AVV wird der Verantwortliche mündliche Weisungen unverzüglich in Textform bestätigen.

3.2 In Bezug auf Klausel 7.1. (b) der AVV hat der Auftragsverarbeiter bei der Information an den Verantwortlichen in Textform mitzuteilen, gegen welche Vorschriften die Befolgung der Weisung seiner Ansicht nach verstößt. Der Verantwortliche wird die beanstandete Weisung entweder abändern oder bestätigen und der Auftragsverarbeiter wird diese Weisung befolgen.

### 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.