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 SD-WAN**" Leistung („**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 SD-WAN** 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 Business SD-WAN** 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 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 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.

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

Diese Klausel wurde absichtlich leer gelassen

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.

(e) *Diese Klausel wurde absichtlich leer gelassen*

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.

ABSCHNITT III
SCHLUSSBESTIMMUNGEN

Klausel 10

Beendigung des Vertrags

(a) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

Die nachstehend aufgeführten Anhänge sind Bestandteil dieser Klauseln:

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

ANHANG I

Liste der Parteien

Verantwortliche(r):

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

Auftragsverarbeiter:

1.4	**Name und Anschrift** *Name und Anschrift des Auftragsverarbeiters*	Telefónica Germany GmbH & Co. OHG Georg-Brauchle-Ring 50 80992 München
1.5	**Kontaktmöglichkeiten für Datenschutzanfragen und zum Datenschutzbeauftragten**	datenschutz@telefonica.com

ANHANG II.a

Dieser Anhang findet ausschließlich Anwendung für den Fall, dass der Kunde die Produktlösung „O_2 Business SD-WAN" des Herstellers FORTINET ausgewählt hat.

BESCHREIBUNG DER VERARBEITUNG

2.1.	**Beschreibung der konkreten Datenverarbeitung (Gegenstand, Art und Umfang)**	Der Auftragsverarbeiter betreibt das unter dem Namen **O_2 Business SD-WAN** bekannte Sicherheitsprodukt des Produktherstellers FORTINET zur Verfügung. Hierbei kann über eine softwaregesteuerte Plattform die zentraler Steuerung, Konfiguration und Überwachung von Netzwerkressourcen gewährleistet werden. Das Software-Defined Wide Area Network (nachfolgend: „SD-WAN" genannt) ist eine softwarebasierte Netzwerktechnologie, die virtualisierte Ressourcen bereitstellt, um Computernetzwerke des Auftraggebers zu erweitern und Standorte und/oder Rechenzentren des Kunden untereinander zu verbinden. Das Produkt nutzt eine virtuelle Architektur in der Cloud, mit dem der Kunde für seine Standorte beliebige Wege für die Datenübertragung von IP-Paketen, kombinieren kann, um Benutzer über ein SD-WAN mit Anwendungen zu verbinden. Dieser Service ermöglicht es dem Kunden sein Netzwerkmanagement und dessen Sicherheitslösungen durch eine softwaredefinierte Lösung zu vereinheitlichen. Zusätzlich ermöglicht das O_2 Business SD-WAN Netz die zentrale Konfiguration, Überwachung und Verwaltung von LAN-Switches und WLAN Access Point über eine Managementplattform. Das SD-WAN-Netz mit LAN-Switch und WLAN Access Points bietet eine integrierte Lösung zur effizienten Verwaltung von Netzwerken an verschiedenen Standorten. Diese innovative Technologie nutzt die Vorteile der Software-Defined-Networking (SDN)-Prinzipien, um die Netzwerkverwaltung und -kontrolle zu zentralisieren. Durch die intelligente Steuerung des Datenverkehrs und die optimale Nutzung der verfügbaren Bandbreite verbessert das O_2 Business SD-WAN die Leistung, Zuverlässigkeit und Sicherheit der Netzwerke. Die Leistungen des Produktes werden durch vor Ort installierte Hardwarekomponenten an den Kundenstandorten erbracht. Die Einrichtung, Steuerung und Konfiguration der Leistungen erfolgt über ein zentrales, webbasiertes Konfigurationsportal. Für die Einrichtung, Konfiguration und Entstörung stellt der Verantwortliche dem Auftragsverarbeiter notwendige Kundeninformationen zur Verfügung (Standortadressen, Konfigurationsdaten, Kundenkontaktdaten). Der Auftragsverarbeiter stellt dem Kunden die Zugangsdaten und erforderliche Logins zum webbasierten Konfigurationsportal zur Verfügung. Der Auftragsverarbeiter wird hierbei Zugang zu personenbezogenen Daten des Kunden nur in dem Umfang nutzen, als dies für die in diesen Abschnitten dieses Anhangs beschriebenen Zwecke erforderlich ist.
2.2.	**Hauptvertrag:** **Geplante Dauer des Auftrags**	Vertrag O_2 Business SD-WAN (Auftragsformular) ☒ befristet bis: Beendigungszeitpunkt des o. g. Hauptvertrages
2.3	**Zweck(e),** die der Tätigkeit des	**1. Zwecke bezüglich Teilnehmer (Kunde eines TK-Dienstes) / Nutzer (Nutzer des TK-Dienstes, der selbst nicht Kunde ist)**

	Auftragsverarbeiters dienen	☒ Gestaltung und/ oder Erbringung eines Telekommunikationsdienstes (z.B. Netzbetrieb) ☒ Verwendung für die Bereitstellung von Diensten mit Zusatznutzen (z.B. location based services) **2. Zwecke bezüglich IT-Leistungen** ☒ Software-/ Systembetrieb ☒Bereitstellung, Betrieb, Betreuung des SD-WAN Netzwerks ☒ Identifizierung und Beseitigung von Störungen und Fehlern
2.4	**Kategorien von Daten**, die durch den Auftrags-verarbeiter verarbeitet werden	**1. Daten bezüglich Teilnehmer (Kunde eines TK-Dienstes) / Nutzer (Nutzer des TK-Dienstes, der selbst nicht Kunde ist)** ☒ Informationen zu genutzter Hardware oder installierter Software (z.B. Geräte-ID, IMEI, TAC) **2. Daten bezüglich Mitarbeiter** ☒ Berufliche Kontaktdaten von Mitarbeitern, Zeitarbeitern, Praktikanten, Auszubildenden (u.a. berufliche Telefonnummer/ E-Mail-Adresse) ☒ Nutzerkennungen (z.B. Login-Daten, Benutzername und Passwort)
2.5	Folgende Daten **betroffener Personen** werden durch den Auftragsverarbeiter verarbeitet	☒ Potenzielle Kunden/ Interessenten ☒ Beschäftigte (z.B. Mitarbeiter/Innen, Praktikanten, Auszubildende) ☒ Sonstiges: O_2 Business SD-WAN Geschäftskunden (die keine anderen TK-Dienstleistungen beziehen)
2.6	Werden bei den vom Auftragsverarbeiter erbrachten Dienstleistungen **sensible Daten** gemäß Ziffer 7.5 verarbeitet?	☒ Nein
2.7	**Kategorien der Datenempfänger**.	☒ Unterauftragsverarbeiter des Auftragsverarbeiters (gilt auch für Konzernunternehmen von Auftragsverarbeitern; Beschreibung der (Unter-) Verarbeitung in **Anhang IV**)
2.8	Standorte, an denen die Daten des Verantwortlichen **gespeichert** werden.	☒ Deutschland ☒ EU/EWR abgesehen von Deutschland (Backup in Irland)
2.9	Standorte, von denen aus auf die Daten des Verantwortlichen wie vorgesehen **zugegriffen** werden kann.	☒ Deutschland ☒ EU/EWR abgesehen von Deutschland
2.10	Ggf. geltende **gesetzliche Verpflichtungen**	Bestehen zum Zeitpunkt des Abschlusses dieses Vertrages entsprechende Verpflichtungen nach dem Recht der Europäischen Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt,

	zur Verarbeitung der für den Verantwortlichen verarbeiteten Daten.	die Daten des Verantwortlichen zu verarbeiten (Art. 28 Abs. 3 S. 2 lit. a DSGVO)? ☒ Nein
2.11	Vorgaben für die **Datenlöschung**.	Die Daten des Verantwortlichen (insbesondere Bestands-/ Verkehrs-/ Inhalts- und Mitarbeiterdaten) sind zu löschen, wenn sie für die Durchführung des Auftrags nicht mehr erforderlich sind, es sei denn es liegt eine abweichende Weisung des Verantwortlichen vor. Die Löschung von Verkehrsdaten hat entsprechend den rechtlichen Anforderungen aus dem "Leitfaden des BfDI und der BNetzA für eine datenschutzgerechte Speicherung von Verkehrsdaten" zu erfolgen. Für die vom Auftragsverarbeiter ausgeführte Speicherung der personenbezogenen Daten des Verantwortlichen gelten die folgenden Höchstspeicherfristen: Die personenbezogenen Daten des Verantwortlichen sind, soweit keine entgegenstehende Einzelweisung erfolgt oder eine gesetzliche oder anderweitige Aufbewahrungspflicht entgegensteht, nach Weitergabe innerhalb von 30 Tagen zu löschen. Spätestens 30 Tage nach Vertragsbeendigung werden die personenbezogenen Daten nach Weisung des Verantwortlichen gelöscht bzw. an den Verantwortlichen herausgegeben und die Kopien gelöscht. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind. 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 II.b

Dieser Anhang findet ausschließlich Anwendung für den Fall, dass der Auftraggeber die Produktlösung „O_2 Business SD-WAN" des Herstellers CISCO Meraki ausgewählt hat.

BESCHREIBUNG DER VERARBEITUNG

2.1.	**Beschreibung der konkreten Datenverarbeitung (Gegenstand, Art und Umfang)**	Der Auftragsverarbeiter betreibt das unter dem Namen **O_2 Business SD-WAN** bekannte Sicherheitsprodukt des Produktherstellers CISCO Meraki zur Verfügung. Hierbei kann über eine softwaregesteuerte Plattform die zentraler Steuerung, Konfiguration und Überwachung von Netzwerkressourcen gewährleistet werden. Das Software-Defined Wide Area Network (nachfolgend: „SD-WAN" genannt) ist eine softwarebasierte Netzwerktechnologie, die virtualisierte Ressourcen bereitstellt, um Computernetzwerke des Auftraggebers zu erweitern und Standorte und/oder Rechenzentren des Kunden untereinander zu verbinden. Das Produkt nutzt eine virtuelle Architektur in der Cloud, mit dem der Kunde für seine Standorte beliebige Wege für die Datenübertragung von IP-Paketen, kombinieren kann, um Benutzer über ein SD-WAN mit Anwendungen zu verbinden. Dieser Service ermöglicht es dem Kunden sein Netzwerkmanagement und dessen Sicherheitslösungen durch eine softwaredefinierte Lösung zu vereinheitlichen. Zusätzlich ermöglicht das O_2 Business SD-WAN Netz die zentrale Konfiguration, Überwachung und Verwaltung von LAN-Switches und WLAN Access Point über eine Managementplattform. Das SD-WAN-Netz mit LAN-Switch und WLAN Access Points bietet eine integrierte Lösung zur effizienten Verwaltung von Netzwerken an verschiedenen Standorten. Diese innovative Technologie nutzt die Vorteile der Software-Defined-Networking (SDN)-Prinzipien, um die Netzwerkverwaltung und -kontrolle zu zentralisieren. Durch die intelligente Steuerung des Datenverkehrs und die optimale Nutzung der verfügbaren Bandbreite verbessert das O_2 Business SD-WAN die Leistung, Zuverlässigkeit und Sicherheit der Netzwerke. Die Leistungen des Produktes werden durch vor Ort installierte Hardwarekomponenten an den Kundenstandorten erbracht. Die Einrichtung, Steuerung und Konfiguration der Leistungen erfolgt über ein zentrales, webbasiertes Konfigurationsportal. Für die Einrichtung, Konfiguration und Entstörung stellt der Verantwortliche dem Auftragsverarbeiter notwendige Kundeninformationen zur Verfügung (Standortadressen, Konfigurationsdaten, Kundenkontaktdaten). Der Auftragsverarbeiter stellt dem Kunden die Zugangsdaten und erforderliche Logins zum webbasierten Konfigurationsportal zur Verfügung. Der Auftragsverarbeiter wird hierbei Zugang zu personenbezogenen Daten des Kunden nur in dem Umfang nutzen, als dies für die in diesen Abschnitten dieses Anhangs beschriebenen Zwecke erforderlich ist.
2.2.	**Hauptvertrag** **Geplante Dauer des Auftrags**	Vertrag O_2 Business SD-WAN (Auftragsformular) ☒ befristet bis: Beendigungszeitpunkt des o. g. Hauptvertrages

2.3	**Zweck(e),** die der Tätigkeit des Auftragsverarbeiters dienen	**1. Zwecke bezüglich Teilnehmer (Kunde eines TK-Dienstes) / Nutzer (Nutzer des TK-Dienstes, der selbst nicht Kunde ist)** ☒ Gestaltung und/ oder Erbringung eines Telekommunikationsdienstes (z.B. Netzbetrieb) ☒ Verwendung für die Bereitstellung von Diensten mit Zusatznutzen (z.B. location based services) **2. Zwecke bezüglich IT-Leistungen** ☒ Software-/ Systembetrieb ☒Bereitstellung, Betrieb, Betreuung des SD-WAN Netzwerks ☒ Identifizierung und Beseitigung von Störungen und Fehlern
2.4	**Kategorien von Daten**, die durch den Auftrags-verarbeiter verarbeitet werden	**1. Daten bezüglich Teilnehmer (Kunde eines TK-Dienstes) / Nutzer (Nutzer des TK-Dienstes, der selbst nicht Kunde ist)** ☒ Informationen zu genutzter Hardware oder installierter Software (z.B. Geräte-ID, IMEI, TAC) **2. Daten bezüglich Mitarbeiter** ☒ Berufliche Kontaktdaten von Mitarbeitern, Zeitarbeitern, Praktikanten, Auszubildenden (berufliche Telefonnummer/ E-Mail-Adresse, Abteilungszugehörigkeit) ☒ Nutzerkennungen (z.B. Login-Daten, Benutzername und Passwort)
2.5	Folgende **Daten betroffener Personen** werden durch den Auftragsverarbeiter verarbeitet	☒ Potenzielle Kunden/ Interessenten ☒ Beschäftigte (z.B. Mitarbeiter/Innen, Praktikanten, Auszubildende) ☒ Sonstiges: O_2 Business SD-WAN Geschäftskunden (die keine anderen TK-Dienstleistungen beziehen)
2.6	Werden bei den vom Auftragsverarbeiter erbrachten Dienstleistungen **sensible Daten** gemäß Ziffer 7.5 verarbeitet?	☒ Nein
2.7	Kategorien der Datenempfänger.	☒ Unterauftragsverarbeiter des Auftragsverarbeiters (gilt auch für Konzernunternehmen von Auftragsverarbeitern; Beschreibung der (Unter-) Verarbeitung in **Anhang IV**)
2.8	Standorte, an denen die Daten des Verantwortlichen **gespeichert** werden.	☒ Deutschland ☒ EU/EWR abgesehen von Deutschland (Cisco Meraki EU Cloud - Dublin)
2.9	Standorte, von denen aus auf die Daten des Verantwortlichen wie vorgesehen **zugegriffen** werden kann.	☒ Deutschland ☒ EU/EWR abgesehen von Deutschland (Cisco Meraki EU Cloud - Dublin)

2.10	Ggf. geltende **gesetzliche Verpflichtungen zur Verarbeitung** der für den Verantwortlichen verarbeiteten Daten.	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	Vorgaben für die **Datenlöschung**.	Die Daten des Verantwortlichen (insbesondere Bestands-/ Verkehrs-/ Inhalts- und Mitarbeiterdaten) sind zu löschen, wenn sie für die Durchführung des Auftrags nicht mehr erforderlich sind, es sei denn es liegt eine abweichende Weisung des Verantwortlichen vor. Die Löschung von Verkehrsdaten hat entsprechend den rechtlichen Anforderungen aus dem "Leitfaden des BfDI und der BNetzA für eine datenschutzgerechte Speicherung von Verkehrsdaten" zu erfolgen. Für die vom Auftragsverarbeiter ausgeführte Speicherung der personenbezogenen Daten des Verantwortlichen gelten die folgenden Höchstspeicherfristen: Die personenbezogenen Daten des Verantwortlichen sind, soweit keine entgegenstehende Einzelweisung erfolgt oder eine gesetzliche oder anderweitige Aufbewahrungspflicht entgegensteht, nach Weitergabe innerhalb von 30 Tagen zu löschen. Spätestens 30 Tage nach Vertragsbeendigung werden die personenbezogenen Daten nach Weisung des Verantwortlichen gelöscht bzw. an den Verantwortlichen herausgegeben und die Kopien gelöscht. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind. 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.a - Technische und organisatorische Maßnahmen des Auftragsverarbeiters, einschließlich zur Gewährleistung der Sicherheit der Daten

Dieser Anhang findet ausschließlich Anwendung für den Fall, dass der Kunde die Produktlösung „O_2 Business SD-WAN" des Herstellers FORTINET ausgewählt hat.

	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	☒	☐	☒	☒

Aktive Speicherung personenbezogener Daten auf den Systemen des Auftragsverarbeiters oder dessen Unterauftragsverarbeiter: ☒ Ja

3.1	Liegt ein **Sicherheitskonzept** gemäß Art. 32 DS-GVO vor?	☒ Ja Weitere Maßnahmen ☒ Durchgeführte Sicherheitsmaßnahmen sind immer auf dem Stand der Technik gehalten
3.2	Sind Maßnahmen zur **Pseudonymisierung** personenbezogener Daten ergriffen worden?	☒ Nein: Gemäß der technisch-organisatorischen Maßnahmen (toM) sind keine Maßnahmen zur Pseudonymisierung von personenbezogenen Daten ergriffen worden, da der Auftragnehmer diese zur Erfüllung des Auftrages benötigt.
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: Der Service wird über einen angemieteten externen Server (geografischer Serverstandort: Europa) gehostet. Es gibt keine Möglichkeit des Zutritts.
3.4	Sind Maßnahmen zur **Zugangskontrolle** ergriffen worden, die gewährleisten, dass ein Zugang durch Unbefugte auf Datenverarbeitungssysteme verhindert wird?	☒ Ja 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 (bspw. passwortgeschützter Bildschirm-schoner) ☒ Dokumentation administrativer Passwörter in gesicherten Passwortsafes ☒ Sichere Verwaltung und Verwendung von digitalem Schlüsselmaterial (z.Bsp.: digitale Zertifikate, Token, etc.) ☒ Regelmäßige Softwareaktualisierung / Patching (Patchmanagement) ☒ Regelmäßige Schwachstellenscans ☒ Netzwerksegmentierung
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 Maßnahmen: ☒ Angemessene Berechtigungskonzepte ☒ Verantwortlichkeiten ☒ Aufgabenbezogene Profile und Rollen ☒ Sollrollenkonzept ☒ Regelmäßige Prüfung der Aktualität von Zugriffsrechten (Rezertifizierung)
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 Maßnahmen: ☒ Gesichertes WLAN ☒ SSL-/TLS-Verschlüsselung ☒ Verwaltung kryptographischer Schlüssel

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 Maßnahmen: ☒ Berechtigungskonzepte vorhanden, inkl.: ☒ Funktionale Verantwortlichkeiten ☒ Angemessene 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 verarbeitet werden können?	☒ Ja Maßnahmen: ☒ Regelmäßige Datenschutzaudits des betrieblichen Datenschutzbeauftragten ☒ Nutzung eines risikoorientierten Auditansatzes ☒ 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
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 Maßnahmen: ☒ Service Level Agreements (SLAs) mit Dienstleistern ☒ Backup Verfahren ☒ Sichere Aufbewahrung für Backups (z.B. Safe, getrennter Brandabschnitt) ☒ Redundante Komponenten (z.B. Spiegeln von Festplatten) ☒ Redundante Versorgung (z.B. Internet, Telefon, Strom) ☒ Schutz der relevanten Infrastruktur gegen Defekte durch äußere Einflüsse ☒ 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 Maßnahmen: ☒ Getrennte Datenbanken
3.11	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

		☒ Regelmäßige Durchführung und Dokumentation von Notfalltests
3.12	Sind Maßnahmen für **Logging** in den relevanten Bereichen ergriffen worden?	☒ Ja ☒ Nutzung von Sicherheits-/Protokollierungssoftware ☒ 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 **Zugangskontrolle** ☒ Logging der Zugänge ☒ Personenbezogenes Logging: Das O2 Business SD-WAN Portal protokolliert fehlgeschlagene Login-Versuche eines Benutzers **Zugriffskontrolle** Logging der Zugriffe ☒ lesend ☒ schreibend
3.13	Ist Mitarbeitern erlaubt aus dem **Homeoffice** zu arbeiten? Sind Maßnahmen zur Arbeit im Homeoffice bzw. für Telearbeit ergriffen worden?	☒ Ja ☒ Homeoffice Richtlinie / Richtlinie mobiles Arbeiten ☒ Verschlüsselung der Remoteverbindung

ANHANG III.b - Technische und organisatorische Maßnahmen des Auftragsverarbeiters, einschließlich zur Gewährleistung der Sicherheit der Daten

Dieser Anhang findet ausschließlich Anwendung für den Fall, dass der Auftraggeber die Produktlösung „O_2 Business SD-WAN" des Herstellers CISCO Meraki ausgewählt hat.

	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	☒	☐	☒	☒

Aktive Speicherung personenbezogener Daten auf den Systemen des Auftragsverarbeiters oder dessen Unterauftragsverarbeiter: ☒ Ja

3.1	Liegt ein **Sicherheitskonzept** gemäß Art. 32 DS-GVO vor?	☒ Ja Weitere Maßnahmen ☒ Durchgeführte Sicherheitsmaßnahmen sind immer auf dem Stand der Technik gehalten
3.2	Sind Maßnahmen zur **Pseudonymisierung** personenbezogener Daten ergriffen worden?	☒ Nein: Gemäß der technisch-organisatorischen Maßnahmen (toM) sind keine Maßnahmen zur Pseudonymisierung von personenbezogenen Daten ergriffen worden, da der Auftragnehmer diese zur Erfüllung des Auftrages benötigt.
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: Der Service wird innerhalb der CISCO Meraki EU-Cloud (geografischer Standort: Europa) gehostet. Es gibt keine Möglichkeit des Zutritts.
3.4	Sind Maßnahmen zur **Zugangskontrolle** ergriffen worden, die gewährleisten, dass ein Zugang durch Unbefugte	☒ Ja Maßnahmen: ☒ Benutzer haben einen eindeutigen persönlichen Bezeichner ☒ Getrennte Benutzerkennungen für privilegierte Berechtigungen

	auf Datenverarbeitungssysteme verhindert wird?	☒ 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 (bspw. passwortgeschützter Bildschirmschoner) ☒ Dokumentation administrativer Passwörter in gesicherten Passwortsafes ☒ Sichere Verwaltung und Verwendung von digitalem Schlüsselmaterial (z.Bsp.: digitale Zertifikate, Token, etc.) ☒ Regelmäßige Softwareaktualisierung / Patching (Patchmanagement) ☒ Regelmäßige Schwachstellenscans ☒ Netzwerksegmentierung
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 Maßnahmen: ☒ Angemessene Berechtigungskonzepte ☒ Verantwortlichkeiten ☒ Aufgabenbezogene Profile und Rollen ☒ Sollrollenkonzept ☒ Regelmäßige Prüfung der Aktualität von Zugriffsrechten (Rezertifizierung)
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 Maßnahmen: ☒ Gesichertes WLAN ☒ SSL-/TLS-Verschlüsselung ☒ Verwaltung kryptographischer Schlüssel

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 Maßnahmen: ☒ Berechtigungskonzepte vorhanden, inkl.: ☒ Funktionale Verantwortlichkeiten ☒ Angemessene 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 verarbeitet werden können?	☒ Ja Maßnahmen: ☒ Regelmäßige Datenschutzaudits des betrieblichen Datenschutzbeauftragten ☒ Nutzung eines risikoorientierten Auditansatzes ☒ 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
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 Maßnahmen: ☒ Service Level Agreements (SLAs) mit Dienstleistern ☒ Backup Verfahren ☒ Sichere Aufbewahrung für Backups (z.B. Safe, getrennter Brandabschnitt) ☒ Redundante Komponenten (z.B. Spiegeln von Festplatten) ☒ Redundante Versorgung (z.B. Internet, Telefon, Strom) ☒ Schutz der relevanten Infrastruktur gegen Defekte durch äußere Einflüsse ☒ 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 Maßnahmen: ☒ Getrennte Datenbanken
3.11	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

		☒ Regelmäßige Durchführung und Dokumentation von Notfalltests
3.12	Sind Maßnahmen für **Logging** in den relevanten Bereichen ergriffen worden?	☒ Ja ☒ Nutzung von Sicherheits-/Protokollierungssoftware ☒ 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 **Zugangskontrolle** ☒ Logging der Zugänge ☒ Personenbezogenes Logging: Das O2 Business SD-WAN Portal protokolliert fehlgeschlagene Login-Versuche eines Benutzers **Zugriffskontrolle** Logging der Zugriffe ☒ lesend ☒ schreibend
3.13	Ist Mitarbeitern erlaubt aus dem **Homeoffice** zu arbeiten? Sind Maßnahmen zur Arbeit im Homeoffice bzw. für Telearbeit ergriffen worden?	☒ Ja ☒ Homeoffice Richtlinie / Richtlinie mobiles Arbeiten ☒ Verschlüsselung der Remoteverbindung

ANHANG IV.a – LISTE DER UNTERAUFTRAGSVERARBEITER

Dieser Anhang findet ausschließlich Anwendung für den Fall, dass der Auftraggeber die Produktlösung „O_2 Business SD-WAN“ des Herstellers FORTINET ausgewählt hat.

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

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

Angabe des Unterauftragsverarbeiters	**Beschreibung der Verarbeitung**	**Bestehen Verträge zur Auftragsverarbeitung zwischen dem Auftragsverarbeiter und Unterauftragsverarbeiter (Art. 28 Abs. 4 DSGVO)?**	**Findet eine Übermittlung oder ein Zugriff auf die Daten des Verantwortlichen in/aus Drittländern (außerhalb der EU/des EWR) statt?**	**Bitte nur im Falle eines Datenzugriffs aus /einer Datenübermittlung in ein Drittland beantworten: Hat der Auftragsverarbeiter gesetzlich vorgeschriebene Garantien und, soweit relevant, Supplementary Measures (vgl. EDPB, Empfehlungen 01/2020[1]) gemäß Kapitel V der DSGVO vorgesehen?**
Name/Firma: Telefónica Cybersecurity & Cloud Tech Deutschland GmbH **Adresse:** Adalperostraße 82-86 85737 Ismaning Deutschland **Ort der Speicherung/ des bestimmungsgemäßen Zugriffs auf die im Auftrag verarbeiteten Daten:** EU	Bereitstellung, Betrieb und Betreuung der SD-WAN-Dienste und Services	☒ 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

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

ANHANG IV.b – LISTE DER UNTERAUFTRAGSVERARBEITER

Dieser Anhang findet ausschließlich Anwendung für den Fall, dass der Auftraggeber die Produktlösung „O_2 Business SD-WAN“ des Herstellers CISCO Meraki ausgewählt hat.

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

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

Angabe des Unterauftragsverarbeiters (dazu gehören auch Konzerngesellschaften), die mit der Auftragsdatenverarbeitung beauftragt werden und möglicherweise Zugriff auf die personenbezogenen Daten des für die Verarbeitung Verantwortlichen haben:	**Beschreibung der Verarbeitung**	**Bestehen Verträge zur Auftragsverarbeitung zwischen dem Auftragsverarbeiter und Unterauftragsverarbeiter (Art. 28 Abs. 4 DSGVO)?**	**Findet eine Übermittlung oder ein Zugriff auf die Daten des Verantwortlichen in/aus Drittländern (außerhalb der EU/des EWR) statt?**	**Bitte nur im Falle eines Datenzugriffs aus /einer Datenübermittlung in ein Drittland beantworten: Hat der Auftragsverarbeiter gesetzlich vorgeschriebene Garantien und, soweit relevant, Supplementary Measures (vgl. EDPB, Empfehlungen 01/2020[2]) gemäß Kapitel V der DSGVO vorgesehen?**
Name/Firma: Telefónica Cybersecurity & Cloud Tech Deutschland GmbH **Adresse:** Adalperostraße 82-86 85737 Ismaning Deutschland **Ort der Speicherung/ des bestimmungsgemäßen Zugriffs auf die im Auftrag verarbeiteten Daten:** EU	Bereitstellung, Betrieb und Betreuung der SD-WAN-Dienste und Services	☒ 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] Empfehlungen 01/2020 zu “Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene” des European Data Protection Board (EDPB), angenommen am 18. Juni 2021

ANHANG V ERGÄNZENDE REGELUNGEN ZUM AVV

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

1. Mobiles Arbeiten

Die Verarbeitung von personenbezogenen Daten des Verantwortlichen außerhalb der Betriebsstätte des Auftragsverarbeiters (z.B. bei mobilem Arbeiten oder bei 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.

2. Vertragsstrafe, Haftung

Die Haftungs- und Schadensersatzvereinbarungen aus dem Hauptvertrag, soweit sie getroffen wurden, finden auf diesen Annex Anwendung.

3. Sonstige Bestimmungen

3.1 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.

3.2 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.

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