Annex Auftragsverarbeitung

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 IT Protect Leistung („**Hauptvertrag**“) ergeben. Für diesen Annex gelten die Begriffsbestimmungen der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) („DSGVO“), sofern nichts Abweichendes bestimmt wurde.

Im Rahmen der Nutzung des von der Telefónica Germany GmbH & Co. OHG bereitgestellten Dienst O_2 Business IT Protect 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 IT Protect i.S.d. Art. 4 Nr. 7 DSGVO verantwortlich.

Klausel 1 - Zweck und Anwendungsbereich

(a) Diese AVV gilt für die Verarbeitung personenbezogener Daten gemäß Anhang II.
(b) Die Anhänge I bis V sind Bestandteil der Klauseln.

Klausel 2 - 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 3 - 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 4 - Pflichten der Parteien

4.1. 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 DSGVO oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

4.2. 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.

4.3. Dauer der Verarbeitung personenbezogener Daten

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

(a) Die Laufzeit dieses Vertrages entspricht – sofern ein Hauptvertrag geschlossen wurde – der im Hauptvertrag vereinbarten Laufzeit. Dieser Vertrag endet mit dem Hauptvertrag, ohne dass es einer separaten Kündigung dieses Vertrages bedarf. Die Parteien können diesen Vertrag nur mit dem zugrunde liegende Hauptvertrag kündigen; sofern im Hauptvertrag nichts Abweichendes vereinbart wurde.

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

4.4. 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.

4.5. Einsatz von Unterauftragsverarbeitern

(a) Der Auftragsverarbeiter darf weitere Auftragsverarbeiter (im Folgenden: „Subunternehmer“) in Anspruch nehmen. Die zum Zeitpunkt des Vertragsschlusses in Anspruch genommenen Subunternehmer sind in Anhang IV zu diesem Vertrag aufgeführt. Der Auftragsverarbeiter hat den Verantwortlichen schriftlich, was auch in einem elektronischen Format erfolgen kann, über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Subunternehmern zu informieren. Gegen derartige Änderungen kann der Verantwortliche nach erfolgter Information durch den Auftragsverarbeiter binnen 14 Tagen Einspruch erheben.

(b) Nimmt der Auftragsverarbeiter die Dienste eines Subunternehmers in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem Subunternehmer im Wege eines Vertrags, der schriftlich abzufassen ist, was auch in einem elektronischen Format erfolgen kann, oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in diesem Vertrag festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DS-GVO erfolgt. Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes Subunternehmers.

Klausel 5 - Haftung

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

Klausel 6 - Unterstützung des Verantwortlichen

(a) Der Auftragsverarbeiter unterstützt den Verantwortlichen angesichts der Art der Verarbeitung mit geeigneten technischen organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DS-GVO genannten Rechte der betroffenen Person nachzukommen (Berücksichtigung von Betroffenenrechten hinsichtlich der Gewährleistung von Transparenz; Recht auf Auskunft; Berichtigungsrecht; Recht auf Löschung („Vergessenwerden“); Recht auf Einschränkung der Verarbeitung; Mitteilungsrecht bei Berichtigung und Löschung sowie Einschränkung der Verarbeitung; Recht auf Datenübertragbarkeit; Widerspruchsrecht; Rechte bei automatisierten Einzelfallentscheidungen).

(b) Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DS-GVO genannten Pflichten (Gewährleistung der Sicherheit der Verarbeitung; Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörden; Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person; Datenschutz-Folgenabschätzung; Vorherige Konsultation).

(c) 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 I

Liste der Parteien

Verantwortlicher:

1.1	**Name und Anschrift**	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 des Auftragsverarbeiters**	Telefónica Germany GmbH & Co. OHG Georg-Brauchle-Ring 50 80992 München
1.5	**Kontaktmöglichkeit für Datenschutzfragen**	datenschutz@telefonica.com

ANHANG II

BESCHREIBUNG DER VERARBEITUNG

2.1.	**Beschreibung der konkreten Datenverarbeitung (Gegenstand, Art und Umfang)**	Die Telefonica Germany GmbH & Co. OHG vermarktet als Auftragsverarbeiter den Managed Service O_2 Business IT Protect, welche in der Basic-Variante die folgenden Produkte und/oder Dienstleistungen enthält: – **Antivirus/ Anti-Ransomware** (basierend auf Lizenzen/Plattform von Musarubra) – **Clean E-Mail** (basierend auf Lizenzen/Plattform von Fortinet): Cloud-Service, der die E-Mail-Kommunikation des Verantwortlichen schützt – **Webbasiertes Kundenportal für die technischen Ansprechpartner des Verantwortlichen** Der Auftragsverarbeiter führt - hauptsächlich über seine Unterauftragsverarbeiter - folgende Verarbeitungstätigkeiten im Auftrag des Verantwortlichen durch und erhält hierzu im erforderlichen Umfang Zugang zu personenbezogenen Daten: - Anlage des Verantwortlichen mit Angabe von ihm benannter Ansprechpartner auf den Plattformen der Produkthersteller - Erstellung von Benutzern und Gewährung des Zugangs zum webbasierten Kundenportal; Benutzer sind Beschäftigte von dem Verantwortlichen (technische Ansprechpartner) - Entgegennahme, Bearbeitung und Lösung von Support-Anfragen der Mitarbeiter des Verantwortlichen. Dies kann die Kommunikation mit den Herstellern, in diesem Fall Musarubra und Fortinet, beinhalten (Third Level Support).
2.2.	**Hauptvertrag** **Geplante Dauer des Auftrags**	Vertrag O_2 Business IT Protect ☐ unbefristet ☒ befristet bis: Beendigung des Hauptvertrages
2.3	**Zweck**	**1. Zwecke bezüglich Teilnehmer (Kunde eines TK-Dienstes) / Nutzer (Nutzer des TK-Dienstes, der selbst nicht Kunde ist)** ☐ Begründung (z.B. Bereitstellung Webshop), inhaltliche Ausgestaltung (z.B. Änderungen des Vertrags, Versand von Rechnungen), Beendigung eines Vertragsverhältnisses mit Teilnehmern, Beratung von Kunden (z.B. Kundenservice) ☐ Gestaltung und/ oder Erbringung eines Telekommunikationsdienstes (z.B. Netzbetrieb) ☐ Ermittlung des Entgelts und Abrechnung mit den Teilnehmern (z.B. Rechnungs-/ EVN-Erstellung) ☐ Verwendung für die Bereitstellung von Diensten mit Zusatznutzen (z.B. location based services) ☐ Verwaltung von Teilnehmerdaten (z.B. Betrieb eines CRM-Systems) ☐ Werbung für Angebote des Verantwortlichen ☐ Werbung für Angebote Dritter ☐ Befragungen im Rahmen von Markt- und Meinungsforschung

		☐ Analyse/ Auswertung für Zwecke der bedarfsgerechten Gestaltung von Telekommunikations- und/ oder Telemediendiensten (z.B. BI, Netzwerkausbau) ☐ Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen ☐ Aufdecken sowie Unterbinden von Leistungserschleichungen und sonstigen rechtswidrigen Inanspruchnahmen der Telekommunikationsnetze und -dienste (Fraud) **2. Zwecke bezüglich Mitarbeiter** ☐ Verwaltung von Bewerbungen ☐ Begründung/ Änderung/ Beendigung eines Vertragsverhältnisses mit Mitarbeitern ☐ Lohn- und Gehaltsabrechnung ☐ Reisebuchung und Reisekostenabrechnung ☐ Pflege und Verwaltung von Mitarbeiterdaten ☐ Dokumentation von Arbeitszeiten ☐ Planung und Verwaltung von Fortbildungs- und Trainingsmaßnahmen ☐ Verwaltung von Qualifikationen/ Skillmanagement ☐ Verwaltung von Mitarbeiterbeurteilungen/ Leistungsbewertungen **3. Zwecke bezüglich Gebäudemanagement** ☐ Überwachung betrieblicher Einrichtungen ☐ Verwaltung/ Gewährleistung des Zutrittsschutzes (z.B. Verwaltung/ Protokollierung von Zutrittsberechtigungen, Zutrittskarten) ☐ Videoüberwachung ☐ Gewährleistung der ordnungsgemäßen Akten- und Datenträgervernichtung **4. Zwecke bezüglich IT-Leistungen** ☐ Gewährleistung der Sicherheit der IT (Informationssicherheit) ☐ Verwaltung von Zugangs-/ Zugriffsrechten auf Informations- und Kommunikationstechnik und Unternehmensnetzwerk ☐ Bereitstellung von internen Kommunikationsmitteln (z.B. E-Mail-System, Intranet) ☐ Software-/ Systementwicklung und Testing ☐ Software-/ Systembetrieb ☒ Wartung/ Support (maintenance) **5. Sonstige Zwecke** ☒ Sonstiges*:* Verwaltung von Zugangs-/Zugriffsrechten auf Plattformen/Portalen
2.4	**Datenkategorien**	**1. Daten bezüglich Teilnehmer (Kunde eines TK-Dienstes) / Nutzer (Nutzer des TK-Dienstes, der selbst nicht Kunde ist)** ☐ Bestandsdaten nach dem TKG (Vertragliche Angaben, wie Name, Adresse, Bankverbindung, Geburtsdatum, MSIDSN, IMEI, IMSI, Kundennummer, Rechnungsnummer, E-Mail-Adresse etc.) ☐ Kundenumsätze/ Revenue ☐ Rechnungen ☐ Bank- oder Kreditkartendaten ☐ Legitimationspapiere (Personalausweiskopie, Personalausweisnummer, Reisepass etc.) ☐ Bonitätsinformationen ☐ Kundenhistorie ☐ Kundenkommunikation ☐ Informationen zu genutzter Hardware oder installierter Software (z.B. Geräte-ID, IMEI, TAC)

		☐ Verkehrsdaten (Daten, die einen konkreten Telekommunikationsvorgang betreffen, wie A-Rufnummer, B-Rufnummer, Uhrzeit, Dauer, genutzter Dienst, Call Data Records, Einzelverbindungsnachweis, IP-Adresse, IMEI): ☐ Standortdaten (Daten zur Identifizierung eines Standorts eines Endgeräts, Cell-ID, GPS-Daten) ☐ Inhaltsdaten (Inhalte der Kommunikation, z.B. E-Mail-Inhalte, Gesprächsinhalte, Datenstrom ab OSI-Layer 4, etc.) **2. Daten bezüglich Besucher einer Internetseite, App-Nutzer** ☐ Bestandsdaten nach dem TTDSG (z.B. Name, Anschrift des Nutzers von Websites und Apps, etc.) ☐ Nutzungsdaten nach dem TTDSG (Beginn, Ende, Umfang der jeweiligen Nutzung z.B. von Websites oder Apps, IP-Adresse etc.) ☐ pseudonyme Nutzungsprofile (z.B. aus Cookies, Webanalyse) **3. Daten bezüglich Mitarbeiter** ☒ Berufliche Kontaktdaten von Mitarbeitern, Zeitarbeitern, Praktikanten, Auszubildenden (berufliche Telefonnummer/ E-Mail-Adresse, Abteilungszugehörigkeit) ☐ Mitarbeiter Stammdaten (z.B. Privatanschrift, Bankverbindung, Alter) ☐ Erweiterte Mitarbeiterdaten (z.B. Familienstand, Steuerklasse, Staatsangehörigkeit) ☐ Bewerberdaten (z.B. Bewerbungsunterlagen, Zeugnisse) ☐ Personalnummern/ IDs ☐ Arbeitszeiten ☐ Löhne- und Gehälter bzw. sonstige Compensation & Benefits ☐ Reisebuchungs- und Abrechnungsdaten ☐ Bewertung von Mitarbeiterqualifikationen und -eigenschaften ☐ Informationen zur Arbeitsleistungsbewertung ☐ Schulungsinformationen/ Fortbildungshistorien ☒ Nutzerkennungen (z.B. Login-Daten, Benutzername und Passwort) ☐ Besondere Kategorien personenbezogener Daten (Angaben über eine natürliche Person zu religiösen oder weltanschaulichen Überzeugungen, rassischer oder ethnischer Herkunft, Gewerkschaftszugehörigkeit, Gesundheit, politischen Meinungen, Sexualleben oder sexueller Orientierung sowie genetische Daten oder biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person; Daten, die einem Berufsgeheimnis unterliegen; Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen) ☐ Foto-/ Videoaufnahmen **4. Sonstige Datenarten** ☒ Sonstiges: Informationen aus Session Cookie für das Login auf dem webbasierten Kundenportal
2.5	Die Daten welcher **betroffenen Personen** werden durch den Auftragsverarbeiter verarbeitet?	☐ TK-Dienste-Teilnehmer (Kunde eines TK-Dienstes) ☐ TK-Dienste-Nutzer (Nutzer des TK-Dienstes, der selbst nicht Kunde ist) ☐ Besucher einer Internetseite, App-Nutzer (Nutzer nach dem Telemediengesetz) ☐ Potenzielle Kunden/ Interessenten ☒ Beschäftigte (z.B. Mitarbeiter/Innen, Praktikanten, Auszubildende) ☐ Freie/ externe Mitarbeiter/innen ☐ Bewerber ☐ Besucher ☐ Geschäftspartner (z.B. Lieferanten, Distributoren, Vertriebspartner) ☐ Sonstiges:

2.6	Werden bei den vom Auftragsverarbeiter erbrachten Dienstleistungen **sensible Daten** gemäß Ziffer 7.5 verarbeitet?	☒ Nein ☐ Ja, und zwar folgende sensible Daten ☐ Rassische oder ethnische Herkunft ☐ Politische Meinungen ☐ Religiöse oder weltanschauliche Überzeugungen ☐ Gewerkschaftsmitgliedschaft ☐ Genetische Daten ☐ Biometrische Daten zum Zweck einer eindeutigen Identifizierung einer natürlichen Person ☐ Gesundheitsdaten ☐ Daten über das Sexualleben oder die sexuelle Ausrichtung einer Person ☐ Daten über strafrechtliche Verurteilungen oder Straftaten
2.7	**Kategorien der Datenempfänger**	☒ Unterauftragsverarbeiter des Auftragsverarbeiters (gilt auch für Konzernunternehmen von Auftragsverarbeitern; Beschreibung der (Unter-) Verarbeitung in **Anhang IV**) ☐ Übermittlung an Dritte (nicht Unterauftragsverarbeiter): *Angabe der Empfänger/externe Stelle/Konzerngesellschaft:* ☐ Wirtschaftsprüfer/ Rechtsanwälte ☐ Auskunfteien ☐ Inkasso-Dienstleister ☐ Behörden ☐ Sonstiges ☐ Nicht zutreffend, es werden keine Daten des Verantwortlichen an Unterauftragsverarbeiter oder Dritte übertragen
2.8	Standorte, an denen die Daten des Verantwortlichen **gespeichert** sind.	☒ Deutschland ☒ EU/EWR abgesehen von Deutschland ☐ Drittländer wie folgt (außerhalb des EU/EWR-Raums)
2.9	Standorte, von denen aus auf die Daten des Verantwortlichen wie vorgesehen **zugegriffen** wird.	☒ Deutschland ☒ EU/EWR abgesehen von Deutschland ☐ Drittländer wie folgt (außerhalb des EU/EWR-Raums)
2.10	**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 ☐ Ja, ☐ Ja, aber betreffendes Recht verbietet eine solche Mitteilung wegen eines wichtigen öffentlichen Interesses
2.11	**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. Eine Datenspeicherung erfolgt ausschließlich in den Systemen des Verantwortlichen:

		☐ Ja ☒ Nein, dann gelten für die vom Auftragsverarbeiter ausgeführte Speicherung der personenbezogenen Daten des Verantwortlichen die folgenden Höchstspeicherfristen: Die personenbezogenen Daten des Verantwortlichen sind, soweit keine entgegenstehende Einzelweisung erfolgt oder eine gesetzliche oder anderweitige Aufbewahrungspflicht entgegensteht, nach Weitergabe an den Verantwortlichen und Zweckerreichung zu löschen. Spätestens nach Vertragsbeendigung werden die personenbezogenen Daten nach Weisung des Verantwortlichen gelöscht bzw. an den Verantwortlichen herausgegeben und die Kopien gelöscht. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind. Der Auftragsverarbeiter vernichtet diese Datensätze ohne Aufforderung des Verantwortlichen mit Ablauf der Aufbewahrungspflichten bzw. mit Wegfall der Notwendigkeit der Datenspeicherung zu Sicherheitszwecken. Der Auftragsverarbeiter informiert den Verantwortlichen 15 Werktage vor einer Löschung von im Auftrag gespeicherten Daten nach Vertragsbeendigung in Textform über die geplante Löschung. Wird eine Archivierung **für den Verantwortlichen** durchgeführt? ☒ Nein ☐ Ja

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

3.1	Liegt ein **Sicherheitskonzept** gemäß Art. 32 DS-GVO vor?	☒ Ja Beachtung von internationalen Standards: ☒ Zertifizierung nach ISO 27001 ☒ Sonstiges (z.B. weitere ISO-Zertifizierung, SOX-Compliance) ENS nivel medio
3.2	Sind Maßnahmen zur **Pseudonymisierung** personenbezogener Daten ergriffen worden?	☒ Ja Ein internes Programm ersetzt die identifizierenden Felder in einem Datensatz durch ein oder mehrere Pseudonyme, d.h. fiktive Identifikatoren (in Form von Codes, zufällig generierter Token, Datenstrings, die echt aussehen, es aber nicht sind). ☐ Nein _____
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 Maßnahmen: ☒ Konzept Sicherheitszonen ☒ Schlüsselverwaltung/ Dokumentation der Schlüsselvergabe ☒ Zutrittskontrollsystem, z.B. Ausweisleser (Magnet-/Chipkarten) ☒ Werkschutz/ Pförtner ☒ Sicherheitstüren / -fenster ☒ Gitter vor Fenstern/ Türen ☒ Türsicherungen (elektrische Türöffner, Zahlenschloss, etc.) ☒ Alarmanlage ☒ Videoüberwachung ☒ Wartung wesentlicher Sicherheitszonen nur unter Aufsicht bzw. Wahrung des vier-Augen-Prinzips ☒ Spezielle Schutzvorkehrungen des Serverraums ☒ Abgeschlossene Aktenschränke ☒ Richtlinie für eine aufgeräumte Arbeitsumgebung
3.4	Sind Maßnahmen zur **Zugangskontrolle** ergriffen worden, die gewährleisten, dass ein Zugang durch Unbefugte auf Datenverarbeitungssysteme verhindert wird?	☒ Ja ☐ Nein Maßnahmen: ☒ Benutzer haben einen eindeutigen persönlichen Bezeichner ☒ 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 ☒ Single-Sign-On für die wesentlichen IT-Systeme ☒ Zwei-Faktor-Authentifizierung für kritische Anwendungen ☒ Automatische Sperrung der Clients nach Zeitablauf ohne Useraktivität (bspw. passwortgeschützter Bildschirmschoner) ☒ Dokumentation administrativer Passwörter in gesicherten Passwortsafes

		☒ Regelmäßige Softwareaktualisierung / Patching (Patchmanagement) ☒ Regelmäßige Schwachstellenscans ☒ Netzwerksegmentierung ☒ Firewall, IDS/IPS
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: ☒ Inventarisierung der für den Auftrag relevanten Unternehmenswerte ☒ Angemessene Berechtigungskonzepte ☒ Verantwortlichkeiten ☒ Sollrollenkonzept ☒ Benutzermanagementprozess inkl. Genehmigungsverfahren ☒ 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: ☒ Getunnelte Datenfernverbindungen (VPN = Virtual Private Network) ☒ Gesichertes WLAN ☒ SSL-/TLS-Verschlüsselung ☒ Verschlüsselung von CD/DVD-ROM, externen Festplatten und/oder Laptops ☒ Regelungen zur Datenträgervernichtung, etc.
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: ☒ Inventarisierung der für den Auftrag relevanten Daten ☒ Berechtigungskonzepte vorhanden, inkl.: ☒ Funktionale Verantwortlichkeiten ☒ Need-to-know Prinzip (allgemein) ☒ Angemessene Funktionstrennung
3.8	Sind Maßnahmen zur **Auftragskontrolle** ergriffen worden, die sicherstellen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den	☒ Ja Maßnahmen: ☒ Verbindliche Sicherheitsleitlinien inkl. Verpflichtungen der Mitarbeiter ☒ Schulungen aller zugriffsberechtigten Mitarbeiter ☒ Regelmäßig stattfindende Nachschulungen

	Weisungen des Verantwortlichen verarbeitet werden können?	☒ Prüfungsplanung für interne und externe Audits ☒ Nutzung eines risikoorientierten Auditansatzes ☒ IT-Change Management Prozess ☒ Trennung von Entwicklungs- und Produktivsystemen inkl. geregeltem Transportprozess (production take over) ☒ Durchführung von Funktions- und Benutzerakzeptanztests ☒ Genehmigungs- und Freigabeverfahren ☒ Regeln für die sichere Entwicklung von Software und Systemen sind festgelegt und werden angewandt ☒ Zugriff auf Source-Code / Customizing geschützt (need-to-know Prinzip)
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: ☒ Business Continuity Strategie und Management ☒ Service Level Agreements (SLAs) mit Dienstleistern ☒ Backup Verfahren ☒ Sichere Aufbewahrung für Backups (z.B. Safe, getrennter Brandabschnitt) ☒ Viren-/Schadcodeschutz ☒ Redundante Komponenten (z.B. Spiegeln von Festplatten) ☒ Redundante Versorgung (z.B. Internet, Telefon, Strom) Rechenzentren sind in Bezug auf Stromversorgung und Kommunikation redundant. ☒ Geeignete Archivierungsräumlichkeiten ☒ Schutz der relevanten Infrastruktur gegen Defekte durch äußere Einflüsse
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 Systeme ☒ Getrennte Datenbanken ☒ Trennung durch Zugriffsregelungen
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 ☒ Übergreifender Notfallplan inkl. regelmäßiger Aktualisierung ☒ 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) **Weitergabekontrolle** ☒ Logging der Datenweitergabe und regelmäßige Überprüfung der Logfiles **Verfügbarkeitskontrolle** ☒ Logging der Verfügbarkeit ☒ Regelmäßige Überwachung der Systeme und Logfiles **Zutrittskontrolle** ☒ Logging der Zutritte ☒ Regelmäßiges Monitoring von Zutritten ☒ Auswertung der Logs zur weiteren Verwendung **Zugangskontrolle** ☒ Logging der Zugänge **Zugriffskontrolle** Logging der Zugriffe ☒ lesend ☒ schreibend ☒ Auswertung der Logs zur weiteren Verwendung
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 ☒ Endgerät ist vom Dienstleister verwaltet ☒ Endgerät ist nach dem Stand der Technik geschützt ☒ Regelmäßige Bestätigung der Einhaltung der Homeoffice Richtlinie ☒ Verschlüsselung der Remoteverbindung ☒ Zwei-Faktor-Authentifizierung ☒ Weitere Authentifizierungsmaßnahmen für den Remote-Zugriff*:* VPN ☒ Organisatorische und physische Maßnahmen zur Gewährleistung der Vertraulichkeit ☒ 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:
☒ *Ja* => 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?**
Name/Firma: Telefónica Cybersecurity & Cloud Tech Deutschland GmbH **Anschrift:** Adalperostraße 82- 86, 85737 Ismaning, Deutschland **Name, Position und Kontaktdaten der Kontaktperson:** Unai Gómez Ángel unai.gomezangel@telefonica.com **Ort der Speicherung/ des bestimmungsgemäßen Zugriffs auf die im Auftrag verarbeiteten Daten:** Frankfurt, Deutschland Dublin, Irland	Verarbeitung im Rahmen des O_2 Business IT Protect Dienstes	☒ Ja, Vereinbarungen gemäß Art. 28 Abs. 4 DSGVO bestehen ☐ Nein	☐ Ja, eine Zugriffsmöglichkeit auf diese Daten von außerhalb der EU/des EWR ist nicht technisch ausgeschlossen. ☒ Nein, eine Zugriffsmöglichkeit auf diese Daten von außerhalb der EU/des EWR ist technisch ausgeschlossen.