Annex Auftragsverarbeitung

Im Rahmen der Nutzung des von der Telefónica Germany GmbH & Co. OHG bereitgestellten MDM-Dienstes (Mobile Device Management) werden regelmäßig personenbezogene Daten verarbeitet. Sie sind gemäß gesetzlicher Regelungen dazu verpflichtet, mit der Telefónica Germany GmbH & Co. OHG (nachfolgend Auftragnehmer) einen Vertrag über die Auftragsverarbeitung abzuschließen.

Vertragspartner sind die Telefónica Germany GmbH & Co. OHG, Georg-Brauchle-Ring 50, 80992 München, und der Kunde.

Dieser Annex konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragspartner, die sich aus der Beauftragung des Auftragnehmers („**Hauptvertrag**“) ergeben. Der Annex findet Anwendung auf alle Tätigkeiten, bei denen der Auftragnehmer personenbezogene Daten oder Daten, die dem Fernmeldegeheimnis unterliegen („**Auftraggeber-Daten**“), verarbeitet. Für diesen Annex gelten die Begriffsbestimmungen der EU-Datenschutzgrundverordnung („DSGVO“) sowie des Bundesdatenschutzgesetzes („BDSG“), sofern nichts Abweichendes bestimmt wurde.

§ 1 Vertragsgegenstand, Zweck der Datenverarbeitung, Verantwortlichkeit

(1) Zweck, Art und Umfang der Verarbeitung von Auftraggeber-Daten im Sinne dieses Vertrags sowie die Art der Daten und der Kreis der betroffenen Personen ergeben sich aus den **Anlagen 1 und 2**.

(2) Der Auftraggeber bleibt im Rahmen dieses Vertrages Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich.
(3) Die Inhalte dieses Vertrags gelten auch für Tätigkeiten des Auftragnehmers im Auftrag des Auftraggebers, bei denen ein Zugriff auf Auftraggeber-Daten durch den Auftragnehmer nicht ausgeschlossen werden kann (bspw. Prüfung oder Wartung automatisierter Verfahren oder Datenverarbeitungsanlagen im Auftrag).

§ 2 Dauer des Auftrags
(1) 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.

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

§ 3 Weisungsgebundene Verarbeitung und Mitteilungspflicht bei vermuteten Verstößen

(1) Der Auftragnehmer darf Auftraggeber-Daten nur auf dokumentierte Weisung des Auftraggebers – auch in Bezug auf die Übermittlung von Auftraggeber-Daten an ein Drittland oder eine internationale Organisation – verarbeiten, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Weisungen werden vom Auftraggeber grundsätzlich in Textform (z.B. per E-Mail) erteilt. Soweit eine Weisung ausnahmsweise mündlich erfolgt, wird diese vom Auftraggeber entsprechend in Textform (z.B. per E-Mail) bestätigt.

(3) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf hinweisen, wenn die Befolgung einer vom Auftraggeber erteilten Weisung nach seiner Ansicht gegen die DSGVO oder eine andere Vorschrift über den Datenschutz verstößt.

§ 4 Vertraulichkeits-/ Verschwiegenheitspflicht

Der Auftragnehmer wird zur Durchführung des Vertrages nur Personen beschäftigen, die er zur Vertraulichkeit verpflichtet hat oder die einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

§ 5 Sicherheit der Verarbeitung / Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO

(1) Der Auftragnehmer ergreift alle erforderlichen technischen und organisatorischen Maßnahmen gem. Artikel 32 DSGVO. Diese werden in Anlage 3 spezifiziert.

(2) Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Während der Dauer dieses Auftrags sind diese durch den Auftragnehmer fortlaufend an die Anforderungen dieses Auftrags anzupassen und dem technischen Fortschritt entsprechend weiterzuentwickeln. Das Sicherheitsniveau der hier und in Anlage 3 festgelegten technischen und organisatorischen Maßnahmen darf nicht unterschritten werden.

(3) Der Auftragnehmer verpflichtet sich, Änderungen der technischen und organisatorischen Maßnahmen, die einen wesentlichen Einfluss auf das gewährleistete Sicherheitsniveau haben, als Ergänzung der Anlage 3 schriftlich zu dokumentieren, was auch in einem elektronischen Format erfolgen kann, und dem Auftraggeber zur Kenntnis zu geben.

§ 6 Inanspruchnahme der Dienste weiterer Auftragsverarbeiter

(1) Der Auftragnehmer darf weitere Auftragsverarbeiter (im Folgenden: „Subunternehmer“) in Anspruch nehmen. Die zum Zeitpunkt des Vertragsschlusses in Anspruch genommenen Subunternehmer sind in **Anlage 4** zu diesem Vertrag aufgeführt. Der Auftragnehmer hat den Auftraggeber 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 Auftragnehmer binnen 14 Tagen Einspruch erheben.

(2) Nimmt der Auftragnehmer die Dienste eines Subunternehmers in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Auftraggebers 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 DSGVO erfolgt. Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes Subunternehmers.

§ 7 Mitwirkungs-/ Unterstützungspflichten

Der Auftragnehmer unterstützt den Auftraggeber angesichts der Art der Verarbeitung mit geeigneten technischen organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO 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).

§ 8 Haftung

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

§ 9 Unterstützung bei der Erfüllung von Auftraggeberpflichten

Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO 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).

§ 10 Löschung und Rückgabe von Auftraggeber-Daten

Soweit gesetzliche oder anderweitige Aufbewahrungspflichten nicht entgegenstehen, wird der Auftragnehmer nach Beendigung des Auftrags auf Weisung des Auftraggebers die Auftraggeber-Daten dem Auftraggeber in einer für den Auftraggeber lesbaren und bearbeitbaren Form herausgeben oder die Auftraggeber-Daten löschen.

§ 11 Pflichtennachweis und Unterstützung bei Überprüfungen

Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung. Er ermöglicht Überprüfungen – einschließlich Inspektionen –, die vom Auftraggeber oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, und trägt zu ihrer Durchführung bei. Der Auftragnehmer kann die Einhaltung seiner Pflichten aus Art. 28 DSGVO, insbesondere die Umsetzung der ergriffenen technischen und organisatorischen Maßnahmen auch durch Vorlage von Zertifikaten (IT-Sicherheits- oder Datenschutzaudits z.B. nach BSI-Grundschutz), Prüfberichten von unabhängigen Instanzen (z.B. Datenschutzbeauftragter, Datenschutz-/ Qualitätsauditoren, Wirtschaftsprüfer, Revision, IT-Abteilung) oder Auszügen hieraus nachweisen.

§ 12 Sonstiges, Allgemeines

(1) Die folgenden **Anlagen** sind wesentlicher Bestandteil dieses Vertrages:

- **Anlage 1:** Allgemeine Angaben zum Auftrag sowie zu Gegenstand, Art und Umfang der Datenverarbeitung.
- **Anlage 2:** Festlegung der Zwecke der Verarbeitung der Auftraggeber-Daten sowie der Art der Daten und des Kreises der betroffenen Personen
- **Anlage 3**: Beschreibung der technischen und organisatorischen Maßnahmen, die der Auftragsverarbeiter gemäß § 5 dieses Vertrages eingeführt hat
- **Anlage 4**: Angaben zu Subunternehmern des Auftragnehmers.

(2) Die Regelungen dieses Vertrags gehen abweichenden Regelungen in einem ggf. geschlossenen Hauptvertrag vor, soweit dieser Vertrag nicht ausdrücklich anderes bestimmt.

(3) 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.

Anlage 1: Allgemeine Angaben zum Auftrag sowie zu Gegenstand, Art und Umfang der Datenverarbeitung

1.1	Beschreibung der konkreten Datenverarbeitung (Gegenstand, Art und Umfang)	Telefónica Germany stellt dem Kunden den Service „MDM“ zur Verfügung. Dies umfasst die Bereitstellung eines Mobile Device Management Services mit Anbindung an eine MDM Plattform, Hierfür werden unter anderem die Dienstleister SEVEN PRINCIPLES AG und Solidas Media eingesetzt. Mittels der MDM Plattform der Dienstleister werden mobile Geräte (Smartphones oder Tabletts) von Mitarbeitern der Endkunden verwaltet. Hierbei nutzt ein registrierter Administrator des Endkunden die Plattform Verwaltung für die effiziente Administration der mobilen Endgeräte des Unternehmens (beispielweise zentrale Wartung von Gerätekonfigurationen, Einspielen von Apps etc.) sowie zur Überwachung der Geräte bzgl. Datensicherheit (bspw. Verwaltung des Zugriffs auf Unternehmensdaten durch die mobilen Endgeräte) Um die Verwaltung der Geräte durch die MDM Plattform zu ermöglichen, werden folgende Daten im System gespeichert: - Gerätedaten des Kunden- Hierbei ist ein Kunde in der Regel eine Firma - Daten des Gerätenutzers (Vorname, Nachname, Email) - Gerätenutzer ist in der Regel ein Mitarbeiter des Kunden, kann aber auch beispielsweise ein Fahrzeug sein o.ä. - Administratordaten (Anmeldename und eMail) – Administrator ist in der Regel ein Mitarbeiter des Kunden oder ein vom Kunden beauftragter Service, welcher von Mitarbeitern der Telefónica Germany oder von Telefónica Germany beauftragter Dienstleister ist (Verwaltung der Geräte als Managed Service). Die Dienstleister als Betreiber der Plattform haben mit der Rolle des Super Administrator Zugriff auf die gelisteten personenbezogenen Daten, nehmen aber keine Veränderungen an den personenbezogenen Daten durch, es sei denn auf Anweisung eines weisungsberechtigten Mitarbeiters von Telefónica Germany. Die MDM Plattform wird als Cloud Service dem Kunden durch Telefónica Germany zur Verfügung gestellt.
1.2	E-Mail-Adresse zur Meldung von Datenschutzvorfällen (§ 2 Abs. 7)	Email: datenschutz@telefonica.com
1.3	Betriebsstätte des Auftragnehmers	Anschrift: Telefónica Germany GmbH & Co. OHG Georg-Brauchle-Ring 50 80992 München
1.4	Weisungsbefugte Personen/ Abteilungen gegenüber dem Auftragnehmer	Fachbereich: Business Digital Team E-Mail-Adresse: Business-digital-team@o2.com
	Weisungsempfänger auf Seiten des Auftragnehmers	Fachbereich: Business Digital Team E-Mail-Adresse: Business-digital-team@o2.com
1.5	Hauptvertrag (Purchase Order-/ Vertragsbezeichnung):	Auftragsformular inkl. weiterer Anlagen, sowie ggfls. individueller Rahmenvertrag

1.6	Beginn der Verarbeitung	Nach Unterschrift des Auftragsformulares seitens des Kunden und Bestätigung des Auftrags durch Telefónica Germany GmbH & Co. OHG als Auftragnehmer.
1.7	Geplante Dauer des Auftrags	Maßgeblich ist die gewählte Vertragslaufzeit sowie die einschlägigen Kündigungsfristen

Anlage 2: Festlegung von Zweck der Verarbeitung der Auftraggeber-Daten sowie der Art der Daten und des Kreis der betroffenen Personen

2.1	**Zweck der** Tätigkeit des Auftragnehmers	**Zwecke bezüglich Teilnehmer (Kunde eines TK-Dienstes)/ Nutzer (Nutzer des TK-Dienstes, der selbst nicht Kunde ist)** ☒ Verwendung für die Bereitstellung von Diensten mit Zusatznutzen (z.B. location based services) ☒ Verwaltung von Teilnehmerdaten (z.B. Betrieb eines CRM-Systems) **Zwecke bezüglich Mitarbeitern** ☒ Pflege und Verwaltung von Mitarbeiterdaten **Zwecke bezüglich IT-Leistungen** ☒ Verwaltung von Zugangs-/ Zugriffsrechten auf Informations- und Kommunikationstechnik und Unternehmensnetzwerk ☒ Software-/ Systementwicklung und Testing ☒ Software-/ Systembetrieb ☒ Wartung/ Support (maintenance) **5. Sonstige Zwecke** ☒ Sonstiges*: MDM dient der Verwaltung von mobilen Infrastrukturen (Smartphones Tabletts). Zum Zwecke der Fehlererkennung und Entstörung der Geräte werden Gerätedaten verwaltet*
2.2	**Datenkate-gorien,** die durch den Auftragnehmer verarbeitet werden	**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.) ☒ Informationen zu genutzter Hardware oder installierter Software (z.B. Geräte-ID, IMEI, TAC) ☒ Standortdaten (Daten zur Identifizierung eines Standorts eines Endgeräts, Cell-ID, GPS-Daten) **Daten bezüglich Mitarbeitern** ☒ Berufliche Kontaktdaten von Mitarbeitern, Zeitarbeitern, Praktikanten, Auszubildenden (berufliche Telefonnummer/ E-Mailadresse, Abteilungszugehörigkeit) ☒ Nutzerkennungen (z.B. Login-Daten, Benutzername und Passwort)
2.3	Folgende Daten von **betroffenen Personen** werden durch den Auftrag-nehmer verarbeitet	☒ TK-Dienste-Teilnehmer (Kunde eines TK-Dienstes) ☒ TK-Dienste-Nutzer (Nutzer des TK-Dienstes, der selbst nicht Kunde ist) ☒ Beschäftigte (z.B. Mitarbeiter/Innen, Praktikanten, Auszubildende) ☒ Geschäftspartner (z.B. Lieferanten, Distributoren, Vertriebspartner)
2.4	Folgende Vorgaben für die **Datenlöschung** werden berücksichtigt	Die Auftraggeber-Daten (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 Auftraggebers 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.

Anlage 3: Beschreibung der technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO

	Anforderung	SEVEN PRINCIPLES AG	SOLIDAS Media GmbH
3.1	**Ergebnis der Risikobewertung** Die Bewertung des jeweiligen Risikos erfolgt anhand der Maßstäbe der DSGVO. (Für Telefónica ist dafür eine Schutzbedarfsanalyse mit dem Bereich Corporate Security durchzuführen, bevor die Anlage ab Ziffer 2 ausgefüllt wird.)	Die Vertragspartei hat die datenschutzrechtlichen Risiken für die in ihrem Aufgabenbereich durchgeführte Datenverarbeitung wie folgt definiert: **Risiko bzgl. Vertraulichkeit:** Daten dürfen lediglich von autorisierten Benutzern gelesen bzw. modifiziert werden. Dies gilt sowohl beim Zugriff auf gespeicherte Daten wie auch während der Datenübertragung. ☐ hoch ☒ normal ☐ ausgeschlossen **Risiko bzgl. Integrität:** Daten dürfen nicht unbemerkt und unautorisiert verändert werden. Alle etwaigen Änderungen müssen nachvollziehbar sein (Daten- & Systemintegrität). ☒ hoch ☐ normal ☐ ausgeschlossen **Risiko bzgl. Verfügbarkeit:** Der Zugriff auf die Daten muss innerhalb eines vereinbarten Zeitrahmens gewährleistet werden; Verhinderung von Systemausfällen. ☐ hoch ☒ normal ☐ ausgeschlossen **Risiko bzgl. Belastbarkeit:** Toleranz und Ausgleichsfähigkeit eines Systems gegen Störungen/Angriffe von innen und außen (Widerstandsfähigkeit, Ausfallsicherheit). ☐ hoch ☒ normal ☐ ausgeschlossen	Die Vertragspartei hat die datenschutzrechtlichen Risiken für die in ihrem Aufgabenbereich durchgeführte Datenverarbeitung wie folgt definiert: **Risiko bzgl. Vertraulichkeit:** Daten dürfen lediglich von autorisierten Benutzern gelesen bzw. modifiziert werden. Dies gilt sowohl beim Zugriff auf gespeicherte Daten wie auch während der Datenübertragung. ☐ hoch ☒ normal ☐ ausgeschlossen **Risiko bzgl. Integrität:** Daten dürfen nicht unbemerkt und unautorisiert verändert werden. Alle etwaigen Änderungen müssen nachvollziehbar sein (Daten- & Systemintegrität). ☒ hoch ☐ normal ☐ ausgeschlossen **Risiko bzgl. Verfügbarkeit:** Der Zugriff auf die Daten muss innerhalb eines vereinbarten Zeitrahmens gewährleistet werden; Verhinderung von Systemausfällen. ☐ hoch ☒ normal ☐ ausgeschlossen **Risiko bzgl. Belastbarkeit:** Toleranz und Ausgleichsfähigkeit eines Systems gegen Störungen/Angriffe von innen und außen (Widerstandsfähigkeit, Ausfallsicherheit). ☐ hoch ☒ normal ☐ ausgeschlossen

3.2	Liegt ein **Sicherheitskonzept** gemäß Art. 32 DSGVO vor?	☒ Ja (*bitte Sicherheitskonzept als weitere Anlage diesem Vertrag beifügen*) Beachtung von internationalen Standards: ☒ Zertifizierung nach ISO 27001 Weitere Maßnahmen ☒ Durchgeführte Sicherheitsmaßnahmen sind immer auf dem Stand der Technik gehalten	☒ Nein Beachtung von internationalen Standards: ☒ Sonstiges (z.B. weitere ISO-Zertifizierung, SOX-Compliance): *bitte im Einzelnen aufführen*: ISO 9001 2015 Weitere Maßnahmen ☒ Durchgeführte Sicherheitsmaßnahmen sind immer auf dem Stand der Technik gehalten
3.3	Sind Maßnahmen zur **Pseudonymisierung** personenbezogener Daten ergriffen worden?	☒ Nein, weil *(bitte begründen)*: Daten werden auf den Speichermedien verschlüsselt abgelegt (Data at rest encryption), so dass nur über das Frontend von autorisierten Benutzern auf die entschlüsselten Daten zugergriffen werden kann. Dies ist notwendig, da der Verwendungszweck der Plattform sonst nicht erfüllt werden kann.	☒ Nein, weil *(bitte begründen)*: Er werden keine personenbezogenen Daten auf Systemen des Auftragnehmer gespeichert, welche über den für den Zweck der Abrechnung benötigten Rahmen hinausgehen.
3.4	Sind Maßnahmen zur räumlichen **Zutrittskontrolle** ergriffen worden, die es Unbefugten verwehren, sich den Systemen, Datenverarbeitungsanlagen oder Verfahren physisch zu nähern, mit denen personenbezogene Daten verarbeitet werden?	☒ Ja Maßnahmen: ☒ Konzept Sicherheitszonen ☒ Schlüsselverwaltung/ Dokumentation der Schlüsselvergabe ☒ Zutrittskontrollsystem, z.B. Ausweisleser (Magnet-/Chipkarten) ☒ Werkschutz/ Pförtner ☒ Sicherheitstüren / -fenster ☒ Türsicherungen (elektrische Türöffner, Zahlenschloss, etc.) ☒ Alarmanlage ☒ Videoüberwachung ☒ Spezielle Schutzvorkehrungen des Serverraums ☒ Abgeschlossene Aktenschränke ☒ Richtlinie für eine aufgeräumte Arbeitsumgebung ☒ Sonstiges: *bitte im Einzelnen aufführen*: Detaillierung im Datensicherheitskonzept	☒ Ja Maßnahmen: ☒ Schlüsselverwaltung/ Dokumentation der Schlüsselvergabe ☒ Zutrittskontrollsystem, z.B. Ausweisleser (Magnet-/Chipkarten) ☒ Türsicherungen (elektrische Türöffner, Zahlenschloss, etc.) ☒ Abgeschlossene Aktenschränke ☒ Richtlinie für eine aufgeräumte Arbeitsumgebung ☒ Sonstiges: *bitte im Einzelnen aufführen*: Zugriff auf Server kann nur durch festgelegte IP Adressen erfolgen, zusätzlich sind diese Verbindungen SSL-verschlüsselt.
3.5	Sind Maßnahmen zur **Zugangskontrolle** ergriffen worden, die verhindern, dass ein Zugang durch Unbefugte auf Datenverarbeitungs-systeme verhindert wird?	☒ Ja Maßnahmen: ☒ Benutzer haben einen eindeutigen persönlichen Bezeichner ☒ Getrennte Benutzerkennungen für priviligierte Berechtigungen ☒ Benutzerkennungen werden, wenn die Benutzer das	☒ Ja Maßnahmen: ☒ Benutzer haben einen eindeutigen persönlichen Bezeichner ☒ Getrennte Benutzerkennungen für priviligierte 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 ☒ Single-Sign-On für die wesentlichen IT-Systeme ☒ 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 ☒ Firewall, IDS/IPS ☒ Überwachung der Remote-Wartungszugriffe durch Dienstleister	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 ☒ Firewall, IDS/IPS ☒ Sonstiges: *bitte im Einzelnen aufführen*: Zugriff auf Server kann nur durch festgelegte IP Adressen
3.6	Sind Maßnahmen zur **Zugriffskontrolle** ergriffen worden, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass 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 ☒ Aufgabenbezogene Profile und Rollen ☒ Sollrollenkonzept ☒ Benutzermanagementprozess inkl. Genehmigungsverfahren ☒ Regelmäßige Prüfung der Aktualität von Zugriffsrechten (Rezertifizierung) ☒ Sonstiges: *bitte im Einzelnen aufführen*: Detaillierung im Datensicherheitskonzept	☒ Ja Maßnahmen: ☒ Inventarisierung der für den Auftrag relevanten Unternehmenswerte ☒ Angemessene Berechtigungskonzepte ☒ Verantwortlichkeiten ☒ Aufgabenbezogene Profile und Rollen

3.7	Sind Maßnahmen zur **Weitergabekontrolle** ergriffen worden, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist?	☒ Ja Maßnahmen: ☒ Getunnelte Datenfernverbindungen (VPN = Virtual Private Network) ☒ Gesichertes WLAN ☒ SSL-/TLS-Verschlüsselung ☒ Verschlüsselung von CD/DVD-ROM, externen Festplatten und/oder Laptops ☒ Verwaltung kryptographischer Schlüssel ☒ Diebstahlschutz für mobile Geräte ☒ Regelungen zur Datenträgervernichtung, etc. ☒ Sichere, rückstandsfreie Löschung: *bitte im Einzelnen aufführen*: Lokale Datenhaltung ist im Regelfall nicht vorgesehen. Sollte eine lokale Datenhaltung seitens Telefonica angewiesen werden, dann erfolgt diese auf separater Hardware, welche danach sicher gelöscht wird ☒ Sonstiges*: bitte im Einzelnen aufführen*: Detaillierung im Datensicherheitskonzept, keine lokale Datenhaltung regelmäßig zulässig.	☒ Ja Maßnahmen: ☒ Verschlüsselung von E-Mail (Ende-zu-Ende) ☒ Getunnelte Datenfernverbindungen (VPN = Virtual Private Network) ☒ Gesichertes WLAN ☒ SSL-/TLS-Verschlüsselung ☒ Verschlüsselung von CD/DVD-ROM, externen Festplatten und/oder Laptops ☒ Diebstahlschutz für mobile Geräte ☒ Regelungen zur Datenträgervernichtung, etc. ☒ Sichere, rückstandsfreie Löschung: *bitte im Einzelnen aufführen*: BSI IT Baseline Protection
3.8	Sind Maßnahmen zur **Eingabekontrolle** ergriffen worden, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind?	☒ Ja Maßnahmen: ☒ Inventarisierung der für den Auftrag relevanten Daten ☒ Berechtigungskonzepte vorhanden, inkl.: ☒ Funktionale Verantwortlichkeiten ☒ Need-to-know Prinzip (allgemein) ☒ Angemessene Funktionstrennung ☒ Sonstiges*: bitte im Einzelnen aufführen*: Detaillierung im Datensicherheitskonzept	☒ Ja Maßnahmen: ☒ Berechtigungskonzepte vorhanden, inkl.: ☒ Funktionale Verantwortlichkeiten ☒ Need-to-know Prinzip (allgemein) ☒ Angemessene Funktionstrennung

3.9	Sind Maßnahmen zur **Auftragskontrolle** ergriffen worden, die sicherstellen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können?	☒ Ja Maßnahmen: ☒ Verbindliche Sicherheitsleitlinien inkl. Verpflichtungen der Mitarbeiter ☒ Schulungen aller zugriffsberechtigten Mitarbeiter ☒ Regelmäßig stattfindende Nachschulungen ☒ Betriebshandbücher für den sicheren Betrieb ☒ Regelmäßige Datenschutzaudits des betrieblichen Datenschutzbeauftragten ☒ Prüfungsplanung für interne und externe Audits ☒ Nutzung eines risikoorientierten Auditansatzes ☒ Monitoring & Reporting über neu Identifizierte Risiken / Schwachstellen ☒ IT Change Management Prozess ☒ Trennung von Entwicklungs- und Produktivsystemen inkl. geregeltem Transportprozess (production take over) ☒ Durchführung von Funktions- und Benutzerakzeptanztests ☒ Genehmigungs- und Freigabeverfahren ☒ Regeln für die sichere Entwicklung von Software und Systemen sind festgelegt und werden angewandt ☒ Zugriff auf Source-Code / Customizing geschützt (need-to-know Prinzip) ☒ Sonstiges*: bitte im Einzelnen aufführen*: ITIL konformer Mangementprozess	☒ Ja Maßnahmen: ☒ Verbindliche Sicherheitsleitlinien inkl. Verpflichtungen der Mitarbeiter ☒ Schulungen aller zugriffsberechtigten Mitarbeiter ☒ Regelmäßig stattfindende Nachschulungen ☒ Regelmäßige Datenschutzaudits des betrieblichen Datenschutzbeauftragten ☒ Prüfungsplanung für interne und externe Audits ☒ Nutzung eines risikoorientierten Auditansatzes ☒ Monitoring & Reporting über neu Identifizierte Risiken / Schwachstellen ☒ IT Change Management Prozess
3.10	Sind Maßnahmen zur **Verfügbarkeitskontrolle** ergriffen worden, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind bzw. zügig wiederhergestellt werden können?	☒ Ja Maßnahmen: ☒ Service Level Agreements (SLAs) mit Dienstleistern ☒ Backup Verfahren ☒ Sichere Aufbewahrung für Backups (z.B. Safe, getrennter Brandabschnitt) ☒ Viren-/Schadcodeschutz ☒ Redundante Komponenten (z.B. Spiegeln von Festplatten) ☒ Redundante Versorgung (z.B. Internet, Telefon, Strom)	☒ Ja Maßnahmen: ☒ Sichere Aufbewahrung für Backups (z.B. Safe, getrennter Brandabschnitt) ☒ Redundante Komponenten (z.B. Spiegeln von Festplatten) ☒ Redundante Versorgung (z.B. Internet, Telefon, Strom) *(bitte spezifizieren)*: redundante VoIP TK , redundante Internetverbindung ☒ Schutz der relevanten Infrastruktur gegen Defekte durch äußere Einflüsse

		☒ Geeignete Archivierungsräumlichkeiten ☒ Schutz der relevanten Infrastruktur gegen Defekte durch äußere Einflüsse ☒ Pläne für Ausfall / Notfall / Wiederanlauf etc. (einzelner Komponenten) ☒ Sonstiges*: bitte im Einzelnen aufführen*: Detaillierung im Datensicherheitskonzept	☒ Pläne für Ausfall / Notfall / Wiederanlauf etc. (einzelner Komponenten)
3.11	Sind Maßnahmen zur Einhaltung des **Trennungsgebots** ergriffen worden, die gewährleisten, dass Daten, die zu unterschiedlichen Zwecken erhoben werden, getrennt verarbeitet (z.B. gelöscht) werden können.	☒ Ja Maßnahmen: ☒ Getrennte Datenbanken ☒ Trennung durch Zugriffsregelungen	☒ Nein, weil *(bitte begründen)*: Es werden nur diese Daten gespeichert, welche für Abrechnungszwecke benötigt werden. Insofern ist keine Trennung erforderlich.
3.12	Sind Maßnahmen und Verantwortlichkeiten für den **Umgang mit Informations-sicherheitsvorfällen und Krisensituationen** definiert worden?	☒ Ja Maßnahmen: ☒ Managementprozess für Security Incidents ☒ Managementprozess für datenschutzrelevante Incidents ☒ Definition der Sicherheitsanforderungen in Krisensituation / im Notfall ☒ Übergreifender Notfallplan inkl. regelmäßiger Aktualisierung	☒ Ja Maßnahmen: ☒ Managementprozess für Security Incidents ☒ Managementprozess für datenschutzrelevante Incidents ☒ Übergreifender Notfallplan inkl. regelmäßiger Aktualisierung ☒ Regelmäßige Durchführung und Dokumentation von Notfalltests
3.13	Sind Maßnahmen für **Logging** in den relevanten Bereichen ergriffen worden?	☒ Ja Maßnahmen:☒ 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	☒ Ja Maßnahmen: ☒ Logs sind gegen unberechtigten Zugriff geschützt (Vertraulichkeit) ☒ Logs sind vor unberechtigter Veränderung geschützt (Integrität) ☒ Logs sind vor Verlust geschützt (Verfügbarkeit)

		☒ Regelmäßige Überwachung der Systeme und Logfiles **Zutrittskontrolle** ☒ Logging der Zutritte ☒ Regelmäßiges Monitoring von Zutritten ☒ Auswertung der Logs zur weiteren Verwendung **Zugangskontrolle** ☒ Logging der Zugänge ☒ Personenbezogenes Logging: *bitte spezifizieren, welche für den Auftrag relevanten Daten geloggt werden:* Es erfolgt eine Authentifizierung des Zugriffs über die persönliche Authentifizierung über Zugriffsschlüssel ☒ Auswertung der Logs zur weiteren Verwendung **Zugriffskontrolle** Logging der Zugriffe ☒ schreibend ☒ Regelmäßiges Monitoring von Zugriffen: *bitte spezifizieren, welche Parameter regelmäßig überwacht werden:* Das Logging wird von dem Anwendungssystem zur Verfügung gestellt und die Nutzung ist in Kundenhoheit. Operative Zugriffe auf das Betriebssystem werden über das System Logging protokolliert	
3.14	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 ☒ Untersagung mobiles Arbeiten in öffentlichen Bereichen ☒ Endgerät ist vom Dienstleister verwaltet ☒ Endgerät ist nach dem Stand der Technik geschützt ☒ Verschlüsselung der Remoteverbindung ☒ Organisatorische und physische Maßnahmen zur Gewährleistung der Vertraulichkeit	☒ Ja ☒ Homeoffice Richtlinie / Richtlinie mobiles Arbeiten ☒ Untersagung mobiles Arbeiten in öffentlichen Bereichen ☒ Endgerät ist nach dem Stand der Technik geschützt ☒ Verschlüsselung der Remoteverbindung

Anlage 4: Angaben zu Subunternehmern des Auftragnehmers

Zur Erfüllung des Vertrages/Hauptvertrages werden bzw. wurden Subunternehmer mit der Erbringung eines Teils der Dienstleistung beauftragt:

Angabe des Subunternehmers/ Konzernunternehmen	**Ort der Speicherung/ des bestimmungsgemäßen Zugriffs auf Auftraggeber-Daten** [*falls abweichend von Anschrift des Subunternehmers]*	**Erfolgt eine Datenverarbeitung oder ein Zugang zu Auftraggeber-Daten aus Drittstaaten (außerhalb der EU/ EWR)?** *[z.B. durch Beauftragung von weiteren Dienstleistern durch den beauftragten Subunternehmer]*	**Gegenstand der Unterbeauftragung und verarbeitete Kategorien von Auftraggeber-Daten**	**Abgeschlossener ADV-Vertrag / EU-Standardvertrag** **Der zwischen Auftragnehmer und Subunternehmer abgeschlossene ADV-Vertrag nach Art. 28 DSGVO/ EU Model Clauses ist vor dem Abschluss dieses Vertrags auf Anforderung vorzulegen.**
Name/ Firma: Telefónica Cybersecurity & Cloud Tech Deutschland GmbH Anschrift: Adalperostraße 82-86, 85737 Ismaning, Deutschland	Anschrift: SEVEN PRINCIPLES AG, Rechenzentrum Frankfurt Anschrift: SOLIDAS Media GmbH Plönzeile 17, 12459 Berlin	☐Ja, ☒Nein, ein Zugang zu Auftraggeber-Daten ist ausgeschlossen	Betrieb der MDM Plattform	☒Ja, liegt vor ☐Nein, weil