

Der im Hauptvertrag zum Produkt genannte Kunde (nachfolgend „Auftraggeber“) und die Vodafone GmbH, Ferdinand-Braun-Platz 1, 40549 Düsseldorf (nachfolgend „Vodafone“), zusammenfassend „die Parteien“, vereinbaren im Rahmen dieser Vereinbarung zur Auftragsverarbeitung (nachfolgend „AV“) Folgendes:

1. Anwendungsbereich

Bei der Erfüllung des dieser AV zugrundeliegenden Hauptvertrags erhält Vodafone Zugriff auf personenbezogene Daten, für welche der Auftraggeber datenschutzrechtlich verantwortlich ist (nachfolgend „Auftragsdaten“). Diese AV konkretisiert die Rechte und Pflichten der Parteien bei der Verarbeitung von Auftragsdaten.

2. Auftragsverarbeitung

2.1 Vodafone verarbeitet Auftragsdaten im Auftrag im Sinne des Art. 28 Abs. 1 Datenschutz-Grundverordnung (DSGVO) (nachfolgend „Auftragsverarbeitung“). Der Auftraggeber bleibt für die Rechtmäßigkeit der Verarbeitung der Auftragsdaten verantwortlich. Art. 28 Abs. 3 lit. a DSGVO bleibt unberührt.

2.2 Die Verarbeitung von Auftragsdaten außerhalb der EU oder des EWR (nachfolgend „Drittland“) durch Vodafone erfolgt nur, wenn und soweit die Voraussetzungen gemäß Art. 44 ff. DSGVO erfüllt sind, insbesondere wenn

- (a) es für das betreffende Drittland einen gültigen Angemessenheitsbeschluss der Europäischen Kommission gemäß Art. 45 DSGVO gibt oder
- (b) die Verarbeitung auf Grundlage und nach Maßgabe der jeweils gültigen Standardvertragsklauseln der Europäischen Kommission gemäß Art. 46 DSGVO erfolgt.

2.3 Vodafone führt die Auftragsverarbeitung ausschließlich nach Maßgabe und in dem Umfang der in Anhang 1 dieser AV festgelegten oder in Bezug genommenen Bestimmungen durch.

2.4 Vodafone unterstützt den Auftraggeber bei der Erfüllung von Anfragen und Ansprüchen der von der Auftragsverarbeitung betroffenen natürlichen Personen gemäß Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten soweit erforderlich und Vodafone zumutbar. Ziffer 8 dieser AV bleibt unberührt.

2.5 Der Auftraggeber wird Vodafone unverzüglich über alle die Datenverarbeitung betreffenden Änderungen informieren. Dies gilt insbesondere im Fall gesetzlicher Änderungen, Änderungen in der Rechtsprechung oder im Fall von Hinweisen der Datenschutz- oder sonstiger Behörden.

3. Datenschutzrechtliche Weisungen

3.1 Vodafone wird den datenschutzrechtlichen Weisungen des Auftraggebers zum „Ob?“ der Verarbeitung von Auftragsdaten, insbesondere zur Speicherung, Löschung, Sperrung oder Berichtigung von Auftragsdaten grundsätzlich folgen. Das „Wie?“ der Verarbeitung, insbesondere die Auswahl der Mittel der Verarbeitung und technische und organisatorische Maßnahmen, ist durch die Parteien vertraglich vereinbart. Die datenschutzrechtlichen Weisungen werden anfänglich durch diese AV festgelegt und können durch im Einzelfall erteilte Weisungen geändert, ergänzt oder ersetzt werden (nachfolgend „einzelfallbezogene Weisungen“). Insofern gelten die allgemeinen vertraglichen Bestimmungen zur Änderung oder Erweiterung vertraglicher Pflichten entsprechend. Einzelfallbezogene Weisungen haben mindestens in Textform (zum Beispiel per E-Mail) zu erfolgen. Ziffer 3.2 dieser AV bleibt unberührt.

3.2 Ist Vodafone der Ansicht, dass eine Weisung im Sinne von Ziffer 3.1 dieser AV gegen gesetzliche Vorschriften verstößt, denen Vodafone unterliegt, wird Vodafone den Auftraggeber hierauf hinweisen. Vodafone ist in diesem Fall berechtigt, die Ausführung der betreffenden Weisung bis zur Entscheidung durch den Auftraggeber auszusetzen. Für die Bestätigung der Weisung gilt Ziffer 3.1 dieser AV entsprechend.

3.3 Die mit der Auftragsverarbeitung befassten Mitarbeiter und andere für Vodafone tätige Personen werden die Auftragsdaten nach Maßgabe der in Ziffer 3.1 dieser AV beschriebenen Weisungen verarbeiten.

3.4 Vodafone setzt bei der Durchführung der Arbeiten nur Mitarbeiter ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden.

3.5 Auftragsdaten werden im Einklang mit Art. 28 Abs. 3 lit. a DSGVO unabhängig von den Weisungen des Auftraggebers verarbeitet, soweit Vodafone durch das Recht der Union oder der Mitgliedsstaaten, dem Vodafone unterliegt, hierzu verpflichtet ist. In einem solchen Fall teilt Vodafone dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

4. Datenlöschung

Vodafone wird verarbeitete Auftragsdaten löschen oder vernichten (nachfolgend einheitlich „löschen“), sobald deren Verarbeitung nicht mehr für die Erfüllung des in Ziffer 2.3 dieser AV festgelegten bzw. in Bezug genommenen Zwecks erforderlich ist. Dies gilt insbesondere nach Beendigung der vertragsgegenständlichen Leistungserbringung, soweit keine gesetzlichen Aufbewahrungs- und Speicherpflichten gelten (etwa gemäß §§ 145 bis 147 Abgabenordnung, § 257 Handelsgesetzbuch). In diesen Fällen erfolgt die Löschung am Ende des Aufbewahrungs- beziehungsweise Speicherzeitraums.

5. Technische und organisatorische Maßnahmen zur Daten- und Informationssicherheit

5.1 Vodafone setzt – vorbehaltlich einer einzelfallbezogenen Weisung – die als Anhang 2 dieser AV beigefügten technischen und organisatorischen Maßnahmen zur Daten- und Informationssicherheit um, um ein dem Risiko für die Rechte und die Freiheit der von der Datenverarbeitung betroffenen natürlichen Personen entsprechendes Schutzniveau für die Auftragsdaten zu gewährleisten (Art. 32 DSGVO).

5.2 Vodafone setzt Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Daten- und Informationssicherheit ein (Art. 32 Abs. 1 lit. d DSGVO).

5.3 Vodafone ist berechtigt, die als Anhang 2 dieser AV beigefügten technischen und organisatorischen Maßnahmen zur Daten- und Informationssicherheit von Zeit zu Zeit anzupassen, insbesondere um dem technischen Fortschritt Rechnung zu tragen. Die angepassten Maßnahmen müssen geeignet sein, um ein dem Risiko für die Rechte und die Freiheit der von der Datenverarbeitung betroffenen natürlichen Personen entsprechendes Schutzniveau zu gewährleisten.

5.4 Vodafone gestaltet im Übrigen die innerbetriebliche Organisation und die internen Abläufe so, dass sie den unmittelbar für Vodafone geltenden gesetzlichen Bestimmungen zum Datenschutz gerecht werden.

6. Besondere Vorkommnisse

Wenn Vodafone in Bezug auf die Auftragsdaten eine Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 DSGVO („Datenschutzverletzung“) bekannt wird, meldet Vodafone diese dem Auftraggeber unverzüglich. Die Entscheidung, ob die von Vodafone an den Auftraggeber gemeldete Datenschutzverletzung der für den Auftraggeber zuständigen Aufsichtsbehörde gemeldet und die von der Datenschutzverletzung Betroffenen benachrichtigt werden, obliegt allein dem Auftraggeber. Dies gilt auch für die Vornahme der Meldung an die zuständige Aufsichtsbehörde und die Benachrichtigung der Betroffenen.

7. Beauftragung von weiteren Auftragsverarbeitern

7.1 Der Auftraggeber erteilt Vodafone die allgemeine Genehmigung für den Einsatz weiterer Auftragsverarbeiter. Vodafone wird dem Auftraggeber eine aktuelle Liste der weiteren Auftragsverarbeitern auf Anfrage beim Kundenservice zur Verfügung stellen. Diese Liste enthält Name und Anschrift der weiteren Auftragsverarbeitern sowie eine Beschreibung der von diesen durchzuführenden Verarbeitungen. Die Liste wird dem Auftraggeber erstmals in Ziffer 3 des Anhangs 1 dieser AV zur Verfügung gestellt.

7.2 Beabsichtigt Vodafone einen neuen weiteren Auftragsverarbeiter einzusetzen, wird Vodafone den Auftraggeber hierüber informieren. Widerspricht der Auftraggeber der Einsetzung des neuen weiteren Auftragsverarbeiters nicht gemäß Ziffer 7.3 dieser AV, wird der neue weitere Auftragsverarbeiter eingesetzt.

7.3 Der Auftraggeber ist berechtigt, der Einsetzung neuer weiterer Auftragsverarbeiter durch Vodafone schriftlich innerhalb von zwei Wochen ab Zugang der Information gemäß Ziffer 7.1 dieser AV in Textform zu widersprechen. Der Auftraggeber wird der Einsetzung eines neuen weiteren Auftragsverarbeiters nur aus wichtigem Grund widersprechen. Ziffer 7.4 dieser AV bleibt unberührt. Sofern der Auftraggeber von seinem Einspruchsrecht Gebrauch macht und Vodafone den weiteren Auftragsverarbeiter trotzdem einsetzt, kann der Auftraggeber den Vertrag fristlos kündigen. Dasselbe Recht zur fristlosen Kündigung steht in diesem Fall auch Vodafone zu.

7.4 Vodafone wird weitere Auftragsverarbeiter nur unter Beachtung von Art. 28 Abs. 4 DSGVO einsetzen.

8. Kontrollen durch Aufsichtsbehörden

Soweit Vodafone den Inhalt dieser AV oder besondere Vorkommnisse betreffende Anfragen von Aufsichtsbehörden erhält, wird Vodafone – vorbehaltlich bestehender gesetzlicher Verpflichtungen – entsprechende Auskünfte nicht erteilen und stattdessen den Auftraggeber über die Anfrage informieren. Vodafone ist berechtigt, die anfragende Aufsichtsbehörde über die Weiterleitung der Anfrage an den Auftraggeber zu informieren.

9. Kontroll- und Auskunftsrechte

Sofern sich der Auftraggeber im Rahmen der ihm zustehenden gesetzlichen Rechte von der Einhaltung der in dieser AV festgelegten und in Bezug genommenen Bestimmungen überzeugen möchte, ist Vodafone berechtigt, diese Anforderungen durch die Vorlage einer Selbstauskunft, eines geeigneten Zertifikats, eines durch einen Dritten erstellten Auditberichts oder durch eine andere, entsprechend geeignete schriftliche Dokumentation oder durch Nachweise gemäß Art. 40 bis 42 DSGVO zu erfüllen. Ein Anspruch auf Zutritt zu Geschäftsräumen von Vodafone, Zugang zu Systemen, welche nicht ausschließlich für den Auftraggeber genutzt werden oder Einsicht in vertrauliche, interne Dokumentationen besteht grundsätzlich nicht. Den Parteien steht es frei, im Einzelfall anderslautende Vereinbarungen zu treffen und die Durchführung eines Audits zu vereinbaren. Den Parteien steht es frei, im Einzelfall anderslautende Vereinbarungen zu treffen und die Durchführung eines Audits zu vereinbaren.

10. Schlussbestimmungen

10.1 Sofern zwischen den Parteien wegen der in dieser AV festgelegten oder in Bezug genommenen Leistungen bereits Vereinbarungen zur Verarbeitung personenbezogener Daten im Auftrag bestehen, werden diese Vereinbarungen mit Wirksamkeit dieser AV aufgehoben. Diese AV regelt abschließend die insoweit bestehenden Rechte und Pflichten der Parteien.

10.2 Für diese Vereinbarung gilt das Formerfordernis von Art. 28 Abs. 9 DSGVO.

10.3 Diese AV kommt mit Annahme des dieser AV zugrundeliegenden Hauptvertrages durch Vodafone zustande und wird für die Dauer des Hauptvertrages geschlossen. Ausnahmsweise gilt diese AV über die Beendigung des Hauptvertrages hinaus, sofern und soweit die Verarbeitung von Auftragsdaten im Auftrag des Auftraggebers noch andauert. Dies gilt nicht, soweit eine Datenlöschung nach Ziff. 4 dieser AV allein deshalb unterblieben ist, weil gesetzliche Aufbewahrungs- und Speicherpflichten der Löschung noch entgegenstehen.

10.4 Diese AV unterliegt deutschem Recht. Gerichtsstand für Streitigkeiten aus dieser AV ist Düsseldorf.

10.5 Die in dieser AV festgelegten und in Bezug genommenen Vorschriften gelten vorrangig gegenüber anderen, die Durchführung dieser AV betreffenden vertraglichen Regelungen zwischen den Parteien zur Verarbeitung von Auftragsdaten durch Vodafone.

10.6 Sollten einzelne Teile dieser AV unwirksam sein, so berührt dies die Wirksamkeit der AV im Übrigen nicht.

Anhang 1 zur AV: Dokumentation der Auftragsverarbeitung

Anhang 2 zur AV: Technische und organisatorische Maßnahmen zur Daten- und Informationssicherheit

Anhang 1 zur AV: Dokumentation der Auftragsverarbeitung**1. Art der Leistung** (Mehrauswahl möglich)

☐	(Teil-)Geschäftsprozess-Outsourcing (Kundenservice, Vertrieb, Buchhaltung, Entwicklung, Forderungsmanagement, etc.)
☐	Betrieb (Applikation, System, Komponenten)
☐	Support (Applikation, System, Komponenten)
☐	Hosting (Daten, Applikation, System, Komponenten)
☐	Wartung/Pflege (Applikation, System, Komponenten)
☒	Sonstige: Ziffer 2

2. Gegenstand und Umfang der Verarbeitung von Auftragsdaten

Der Auftraggeber hat bei Vodafone verschiedene Service-Leistungen zu „Vodafone Business UC mit RingCentral“ (nachfolgend „UCaaS“) gebucht. Hierbei handelt es sich um eine cloudbasierte Kommunikationslösung für Unternehmen für Sprach- und Video-konferenzen, Messaging und Teamarbeit. Im Auftrag und auf Weisung des Auftraggebers verarbeitet Vodafone Auftragsdaten im Zusammenhang mit den folgenden Leistungen:

- Soweit nicht iRv Telekommunikationsleistungen (TKL): Support Services und Service-Prozesse (z.B. Incident Management, Eskalationsmanagement)
- Nach Beauftragung (optional):
 - Professional Services** (Einweisung Inbetriebnahme, Implementierungsservice, Migrationsleistungen)
 - Speicherung über die gesetzlichen Fristen für TKL hinaus:** Speicherung der Anrufliste (Anruflisten) und von Anrufaufzeichnungen gemäß der gebuchten Speicherdauer bei UCaaS
 - „RingCX“** als Omnichannel Contact Center Lösung einschließlich Support

RingCX hat folgende KI-Funktionen: die „Sprache in Text Transkription“ (Automated Speech Recognition) von Google LLC sowie die „Zusammenfassung der Konversation für Live Transkriptionen“ (Generate Interactions Summary) durch OpenAI Komponenten, bereitgestellt über Microsoft Azure. Letztere Funktion kann auf Account Level ein- und ausgeschaltet werden.

Auch bei RingCX kann der Auftraggeber die Dauer der Speicherfristen auf Wunsch verlängern (z.B. 90 Tage für Anrufaufzeichnungen, 30 Tage für Faxe, 1 Jahr für Meeting Aufzeichnungen und 5 Minuten für Transkripte von Voice-mails), Anrufaufzeichnungen und Anrufstatistiken sogar bis zu 8 Jahren. Weitere Einzelheiten siehe Hauptvertrag.

3. Weitere Auftragsverarbeiter

Vodafone ist berechtigt, nachfolgend aufgeführte weitere Auftragsverarbeiter einzusetzen:

Name und Anschrift des weiteren Auftragsverarbeiters	Beschreibung der durch den weiteren Auftragsverarbeiter durchzuführenden Verarbeitung von Auftragsdaten
RingCentral Germany GmbH Poststraße 33 20354 Hamburg Deutschland	Support Services und Service-Prozesse, soweit nicht TKL Professional Services Speicherung der Anrufliste (Anruflisten) und Speicherung von Anrufaufzeichnungen gemäß der gebuchten Speicherdauer RingCX
Vodafone Group Services Limited 85 Northbrook Street Newbury RG14 1AE United Kingdom	Migrationsleistungen
Vodafone Shared Services Egypt Smart Village, V-HUB2 (EG100024) VHUB2 Building Smart Village, Alexandria Desert Road Giza 12577, Ägypten	Migrationsleistungen

Die genannten Auftragsverarbeiter beabsichtigen, weitere Auftragsverarbeiter zu beauftragen. Welche dies konkret sind, kann über anfrage.dienstleister@vodafone.com erfragt werden.

4. Ort der Datenspeicherung durch Vodafone oder einen weiteren Auftragsverarbeiter

☒	Bundesrepublik Deutschland
☐	Sonstiges Land innerhalb der EU oder des EWR: -
☒	Drittland, für das ein gültiger Angemessenheitsbeschluss der Europäischen Kommission gemäß Art. 45 DSGVO existiert: United Kingdom (nur bei Beauftragung von Migrationsleistungen)
☐	Sonstiges Drittland: -
☐	Keine Datenspeicherung durch den Auftragsverarbeiter oder einen weiteren Auftragsverarbeiter

Nur bei Beauftragung von **RingCX** sind folgende Orte involviert:

☒	Bundesrepublik Deutschland
☐	Sonstiges Land innerhalb der EU oder des EWR: -
☒	Drittland, für das ein gültiger Angemessenheitsbeschluss der Europäischen Kommission gemäß Art. 45 DSGVO existiert: United Kingdom
☒	Sonstiges Drittland: USA Hinweis: Eine Speicherung erfolgt nur beim Erstellen von Tickets im CRM Support Ticket System von Salesforce.com Inc., 415 Mission Street, 3rd Floor, San Francisco, CA 94105, USA. Gespeichert werden der Name, die E-Mail-Adresse und die Telefon-/Mobilfunknummer des Nutzenden.
☐	Keine Datenspeicherung durch den Auftragsverarbeiter oder einen weiteren Auftragsverarbeiter

5. Ort des Datenzugriffs durch Vodafone oder einen weiteren Auftragsverarbeiter

☒	Aus der Bundesrepublik Deutschland heraus
☒	Aus einem sonstigen Land innerhalb der EU oder des EWR heraus: Bulgarien
☒	Aus einem Drittland heraus, für das ein gültiger Angemessenheitsbeschluss der Europäischen Kommission gemäß Art. 45 DSGVO existiert: United Kingdom (nur bei Beauftragung von Migrationsleistungen)
☒	Aus einem sonstigen Drittland heraus: Ägypten (nur bei Beauftragung von Migrationsleistungen)

Nur bei Beauftragung von **RingCX** sind folgende Orte involviert:

☒	Aus der Bundesrepublik Deutschland heraus: (Tier 2 und 3 Support, Automated Speech Recognition, Generate Interactions Summary)
☒	Aus einem sonstigen Land innerhalb der EU oder des EWR heraus: Bulgarien (Tier 2 und 3 Support), Spanien (Tier 2 (advanced), 3 und Operational Support), Frankreich (Tier 2 und 3 Support)
☒	Aus einem Drittland heraus, für das ein gültiger Angemessenheitsbeschluss der Europäischen Kommission gemäß Art. 45 DSGVO existiert: United Kingdom (Tier 2 und 3 Support, Automated Speech Recognition, Generate Interactions Summary)
☒	Aus einem sonstigen Drittland heraus: USA (Tier 2 (advanced), 3 und Operational Support, CRM Support Ticket System), Philippinen (Tier 2 und Operational Support)

6. Kategorien von Betroffenen

In Abhängigkeit der Nutzung durch den Auftraggeber können im Rahmen der Auftragsverarbeitung insbesondere folgende Kategorien von Betroffenen umfasst sein:

☒	Kunden bzw. Ansprechpartner bei Kunden
☒	Mitarbeiter, Bewerber
☒	Lieferanten bzw. Ansprechpartner bei Lieferanten, sonstigen Dienstleistern und Geschäftspartnern, Freelancer
☒	Sonstige Betroffene, z.B. Interessenten (Kundenseite oder potentielle Geschäftspartner), Kontaktdaten von behördlichen Mitarbeitern, sonstige Dritte

7. Kategorien von Auftragsdaten

In Abhängigkeit von der Nutzung durch den Auftraggeber können im Rahmen der Auftragsverarbeitung insbesondere folgende Kategorien von Auftragsdaten umfasst sein:

☒	Stammdaten , d.h. personenbezogene Daten, die erforderlich sind, um das mit einem Betroffenen bestehende Vertragsverhältnis zu begründen, durchzuführen und ggf. zu beenden (Namen, Vorname, Kunden-, Mitarbeiter- oder Vertragsnummern, Informationen über Produkte, Tarife, Unternehmens- oder Abteilungszugehörigkeit, Rechnungsinformationen, Informationen über Kontakthistorie, etc.)
☒	Kontaktinformationen , d.h. Postadressen, E-Mail-Adressen, Telefonnummer(n), Messenger-IDs, etc.
☐	Bankdaten , d.h. Kontonummer/IBAN, Kreditkarteninformationen
☒	Kommunikationsinhalte , d.h. SMS- oder E-Mail-Inhalte, Voice-Messages, Clickstreams, etc.
☐	Standortdaten aus Netzwerkkommunikation, d.h. Cell-IDs aus Mobilfunkverbindungen, GPS-Koordinaten, IP-Lokalisierung, etc.
☒	Verkehrsdaten (excl. Standortdaten), d.h. Informationen die bei der Initiierung, Aufrechterhaltung und Abwicklung eines konkreten Kommunikationsvorgangs bei Vodafone notwendigerweise anfallen, d.h. z.B. einem Kommunikationsvorgang zuordenbare Anschlusskennungen (A- und B-Rufnummer), IP-Adressen oder Gerätekennungen (MAC-Adresse, IMEI, etc.), Informationen zu Beginn und Ende von Kommunikationsvorgängen (etwa in CDRs oder Log-Dateien)
☒	Endgerätedaten (excl. Standortdaten), d.h. aus Endgeräten, etwa über mobile Apps ausgelesene Informationen (Log-Files, Systemzustände, Nutzereinstellungen, etc., Browserinformationen)
☐	Nutzungsdaten , d.h. Informationen über Art, Umfang, Dauer und Zeitpunkt der Nutzung eines webbasierten Multimedia-Angebots (Webseiten, Videoangebote, etc.)
☒	„User generated content“ , d.h. Inhalte (Dokumente, Bilder, Musikdateien, Äußerungen etc.), die Betroffene willentlich und wissentlich selbst erzeugt haben
☒	User-Account-Informationen , d.h. z.B. Benutzername, Passwort, Rechteprofil, Organisationsinformationen, etc.
☒	Sonstige Daten : ggf. vom Benutzer eingetragene Informationen, wie Weiterleitungsziele oder Urlaubs- / Feiertagspläne
☒	Weitere mögliche Daten bei RingCX : Daten der IT-Applikation (u.a. Anruferaufzeichnungen, E-Mails, Web Browsing History), Cookie-Daten (z.B. Einwilligungsnachweise), Trainingspläne, Incidents und Investigations (z.B. Screenshots, sonstige Nachweise), Daten zur IT-Sicherheit (z.B. Firewall Logs, Webserver Log Files), Daten im Rahmen der Bearbeitung von Behördenanfragen an den Auftraggeber (z.B. Verkehrs- und Standortdaten)

8. Kategorien besonders schützenswerter Auftragsdaten

☐	Daten über die rassische und ethnische Herkunft (z.B. Zugehörigkeit zu einer bestimmten Volksgruppe im Rahmen von Asylverfahren)
☐	Daten über religiöse oder weltanschauliche Überzeugungen (z.B. Informationen über Religionszugehörigkeit im Rahmen der steuerlichen Erfassung)
☐	Genetische Daten (z.B. genetische Veranlagungen bzw. bekannte Erbkrankheiten)
☐	Gesundheitsdaten (z.B. Krankenakten im betriebsmedizinischen Dienst, BEM-Daten, Krankmeldungen)
☐	Daten über politische Meinungen (z.B. Wahlentscheidungen oder Parteizugehörigkeiten)
☐	Daten über die Gewerkschaftszugehörigkeit
☐	Biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person (können in Ausnahmefällen im Rahmen der Wartung/Pflege einsehbar sein)
☐	Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person

Anhang 2 zur AV: Technische und organisatorische Maßnahmen zur Daten- und Informationssicherheit

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1 Zutrittskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pfortner, Alarmanlagen, Videoanlagen.

1.2 Zugangskontrolle

Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern.

1.3 Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen.

1.4 Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing.

1.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur.

2.2 Eingabekontrolle

Feststellung, ob, wann und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

3.1 Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne.

3.2 Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

4.1 Datenschutz-Management

4.2 Incident-Response-Management

4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

4.4 Auftragskontrolle

Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.