Auftragsverarbeitung i.S.d. Art. 28, Abs. 3 Datenschutz-Grundverordnung (DS-GVO)

Fassung AV02_2026

Anlage AV zu bestehenden IT-Aufträgen, IT-Wartungsverträgen und Cloud-Verträgen zwischen

ditpro GmbH & Co. KG, Würzburger Straße 14, 01187 Dresden

(**Auftragnehmer**)

und

Firma: …

Anschrift: …

Ansprechpartner: …

(**Auftraggeber**)

über Auftragsdatenverarbeitung i.S.d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO).

Präambel

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im o.g. Vertrag in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten. Hiermit wird die nachfolgende Anlage AV (Seiten 2-4 zzgl. Anlage 1, 2 und 3) bestätigt und anerkannt.

Ort, Datum, Unterschrift	Ort, Datum, Unterschrift
Auftraggeber	*ditpro GmbH & Co. KG*

§ 1 Gegenstand, Spezifizierung und Dauer der Auftragsverarbeitung

1. Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung. Sofern dies nicht klar hervorgeht, handelt es sich um Installation, Einrichtung, Support und Fehlerbehebung von Server- und Clientbetriebssystemen sowie kunden- und branchenspezifischer Software (CRM, ERP, Online-Banking, usw.) und weiterer, angrenzender Software (Backup, Virenschutz, VPN, Firewall). Der Auftragnehmer erhält im Rahmen dieser Tätigkeiten (Remote-)Zugriff auf die kompletten IT- und Daten-Systeme sowie auf das einzelne Benutzerkonto des Auftraggebers und dessen Mitarbeiter.

Des Weiteren ist der Auftragnehmer auch Service-Provider und stellt Auftraggebern nach Bedarf eine Cloud-Infrastruktur über ein Rechenzentrum zur Verfügung, über welche die mit dem Kunden vertraglich vereinbarten Dienste bzw. Lösungen bereitgestellt werden und auf welcher der Kunde Daten speichern und bearbeiten kann. Hierzu zählen insbesondere der Betrieb der den Service zur Verfügung stellenden Front- und Backendsysteme inklusive der Datenbanksysteme, sowie die Pflege der Hardwaresysteme auf denen die Dienste basieren und der Managed Service für die eingesetzten Softwarelösungen auf den IT-Systemen.

2. Im Einzelnen sind insbesondere die folgenden Daten der in Anlage 2 aufgeführten Tabelle Bestandteil der Datenverarbeitung.

3. Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Anlage nicht darüberhinausgehende Verpflichtungen ergeben.

§ 2 Anwendungsbereich und Verantwortlichkeit

1. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DS-GVO).

2. Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

§ 3 Pflichten des Auftragnehmers

1. Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

2. Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

3. Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten. Ein entsprechendes Angebot hierfür ist im Vorfeld beim Auftragnehmer einzuholen und zu beauftragen.

4. Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

5. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.

Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

6. Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen. Als Datenschutzbeauftragter ist beim Auftragnehmer Herr Kevin Kretzschmar, Würzburger Straße 14, 01187 Dresden, office@ditpro.de, Tel.: 0351-8966690-0 bestellt.

7. Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

8. Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt

der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart. Ein entsprechendes Angebot hierfür ist im Vorfeld beim Auftragnehmer einzuholen und zu beauftragen.

In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart. Ein entsprechendes Angebot hierfür ist im Vorfeld beim Auftragnehmer einzuholen und zu beauftragen.

9. Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

10. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen. Ein entsprechendes Angebot hierfür ist im Vorfeld beim Auftragnehmer einzuholen und zu beauftragen.

§ 4 Pflichten des Auftraggebers

1. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

2. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt §3 Abs. 10 entsprechend. Ein entsprechendes Angebot hierfür ist im Vorfeld beim Auftragnehmer einzuholen und zu beauftragen.

3. Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

§ 5 Anfragen betroffener Personen

1. Wendet sich eine betroffene Person mit Forderungen zur Berichtigung Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 6 Nachweismöglichkeiten

1. Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.

2. Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung verlangen, wenn dies im Vertrag vereinbart ist. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

3. Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§ 7 Subunternehmer (weitere Auftragsverarbeiter)

1. Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.

2. Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.

Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung von Subunternehmern durchgeführt, die in Anlage 3 aufgeführt sind.

3. Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

§ 8 Informationspflichten, Schriftformklausel, Rechtswahl

1. Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher« im Sinne der Datenschutz-Grundverordnung liegen.

2. Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

3. Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

4. Es gilt deutsches Recht.

§ 9 Haftung und Schadensersatz

Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

Anlage 1, Seite 1 – Technisch-organisatorische Maßnahmen
(Version 3.0 vom 04.02.2026)

a) Überblick über die Maßnahmen zur Zutrittskontrolle:
Büros (Würzburger Straße 14, 01187 Dresden und Aurelienstraße 12, 04177 Leipzig):
- Sicherheitsschließanlage für alle Geschäftsräume
- Schlüsselverwaltung zentral nach Protokoll geregelt
- Klare Berechtigungsstrukturen für Zutritt in Archiv-, Büro- und Netzwerkräume
- Büroräume und Schränke stets verschlossen (Zutritt externer Personen nur nach Anmeldung)
- sorgfältige Auswahl von Reinigungspersonal
- Videoüberwachung sicherheitsrelevanter Bereiche

Rechenzentrum (NorthC Deutschland GmbH, Am Tower 5, 90475 Nürnberg):
- 24-Stunden-Wachdienst
- mehrstufige Zutrittskontrollen mit Alarmanlagen, Videoüberwachung, Bewegungssensoren
- Legitimierung der Techniker über Personalausweis und Autorisierung Dritter durch Auftragnehmer

b) Überblick über die Maßnahmen zur Zugangskontrolle:
- authentifizierter Remote-Zugriff auf Systeme des Auftraggebers über TeamViewer, NinjaOne oder VPN mit Kennwortvorgaben und Multifaktor-Authentifizierung (MFA)
- authentifizierter Zugriff auf IT-Dokumentation des Auftraggebers erfolgt nur zu Wartungs- und Supportzwecken und für berechtigte Administratoren
- personalisierter, authentifizierter Zugang auf die Basisplattform im Rechenzentrum ausschließlich per VPN-Verbindung oder mit durch MFA geschützte Fernwartungsverbindungen
- Passwortgeschützte Mitarbeitergeräte mit Vorgaben zu Länge und Komplexität
- Verpflichtende Änderung voreingestellter Standardpasswörter
- es erfolgt keine Weitergabe der Passwörter
- Automatische Bildschirmsperre bei Inaktivität
- Einsatz von Anti-Viren-Programmen und Firewalls, Multifaktorverfahren

c) Überblick über die Maßnahmen zur Zugriffskontrolle:
Allgemein:
- Administratoren mit Zugriffsberechtigung sind namentlich bekannt, durchgeführte Arbeiten mit Datenzugriff werden über das Helpdesk-System des Auftragnehmers dokumentiert
- Rollenkonzept mit abgestuften Berechtigungen, regelmäßige Überprüfung der Rollen
- Anzahl der Administratoren ist auf erforderliches Maß minimiert
- Im Einsatz befindliche IT-Systeme bilden die Systemrechtevergabe durch Rollen ab und erlauben somit die Beachtung von Funktionstrennungsprinzipien
- Verpflichtung aller Administratoren auf Datenschutz und Geheimhaltung
- Mitarbeiter mit Administrationsberechtigungen werden regelmäßig hinsichtlich ihrer Eignung überprüft
- Rechteverwaltung ausschließlich durch Geschäftsführer Technik
- Sichere Aufbewahrung von Datenträgern auch am Arbeitsplatz
- Einsatz von Akten- und Datenträgervernichtung gemäß geltenden Normen
- E-Mail-Transport- und Inhaltsverschlüsselung (S/MIME, sofern unterstützt)

Rechenzentrum:
- Einsatz von VPN- und TLS-Verbindungen für den elektronischen Datenaustausch mit dem Rechenzentrum sowie den Lieferanten des Auftragnehmers
- Einsatz von Transportverschlüsselungstechniken für den Zugriff auf sämtliche Administrationsbereiche von datenhaltenden Systemen
- leistungsstarke Firewall-Funktionen wie Datenverlustprävention (DLP), Verhaltensanalyse und Outbound-Filter verhindern wirksam das unbeabsichtigte Abfließen von Daten

d) Weitergabekontrolle von Daten:
Allgemein:
- ohne Zustimmung keine Weiterleitung von Mails
- kennwortgeschützte Übermittlung von vertraulichen Daten (z.B. Dokumentationen)
- Fernzugriff ausschließlich über verschlüsselte Verbindungen (TeamViewer, NinjaOne, RDP via VPN)
- Festplatten-Vernichtung erfolgt nach BDSG und DIN 66399 in der Sicherheitsstufe H-4, Schutzklasse 2 (hoher Schutzbedarf, Materialteilchenfläche nach der Vernichtung =< 160mm^2)
- Festplatten-Vernichtung wird mit jeder einzelnen Seriennummer dokumentiert und zertifiziert
- die Datenübertragungen zwischen den im Einsatz befindlichen Systemen erfolgt ausschließlich über gesicherte Übertragungswege (bspw. VPN oder HTTPS)
- Datenexporte von personenbezogenen Daten erfolgen nach strikten Prozeduren und können nur von geschulten Administratoren durchgeführt werden
- Für den Datenträgertransport gelten strenge Vorschriften, darunter der Einsatz von Sicherheitstransportbehältern

Rechenzentrum:
- die produktive Datenhaltung erfolgt primär auf den durch den Auftragnehmer eigenverwalteten Systemen innerhalb der RZ-Umgebung. Zusätzlich erfolgt eine veränderungsgeschützte und verschlüsselte Kopie der Datensicherung in das Rechenzentrum des Subunternehmers Elovade in Frankfurt am Main (Deutschland).

e) Eingabekontrolle:
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten über individuelle Benutzerkonten (soweit technisch möglich)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts (soweit technisch möglich)
- Dokumentation aller Datenzugriffe im Helpdesk-System
- Versionierung aller Änderungen an Kundendokumentationen

f) Auftragskontrolle:
Auftragskontrolle bei Auftragsverarbeitung als Auftragnehmer:
- Datenzugriff erfolgt nur im Rahmen der im Auftragsverhältnis notwendigen IT-Arbeiten
- Weisungsbefugnisse und Kontrollrechte des Auftraggebers über die Daten bleiben jederzeit bestehen

Auftragskontrolle bei Auftragsverarbeitung als Auftraggeber:
- sorgfältige Auswahl des Auftragnehmers hinsichtlich der Datensicherheit
- Auftragnehmer hat Datenschutzbeauftragten bestellt
- Auftragsdatenverarbeitungs-Vereinbarungen werden geschlossen
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
- Vereinbarung, dass Anweisungen nur schriftlich erfolgen

Anlage 1, Seite 2 – Technisch-organisatorische Maßnahmen
(Version 3.0 vom 04.02.2026)

g) Verfügbarkeitskontrolle:
Büros:
- Keine Speicherung primärer Kundendaten auf Arbeitsplatzrechnern

Rechenzentrum:
- TÜV- und ISO-zertifiziertes Rechenzentrum (ISO 27001, ISO 9001, ISAE 3402 Type II, ISO 14001, DIN 50600 Cat III, ISO 20000)
- redundante Auslegung der Trafo- und USV-Anlagen (UPS Redundanz: N+1 Generator Redundanz: N+1)
- 2x10 kV (2N) Anschluss an das Energienetz
- voll redundante Klimakreisläufe auf den RZ-Flächen
- sechs Dieselgeneratoren mit je zwei MVA
- Notstromaggregate für hohe Verfügbarkeiten
- komplexe Brandschutzvorrichtungen mit Brandfrüherkennung und VESDA-System und Argon-Löschanlage
- Permanente Umgebungsüberwachung (Temperatur/Feuchte)

IT-Plattform im Rechenzentrum:
- die Hardwareumgebung wird vollständig und ausschließlich durch ditpro verwaltet und betreut
- Markenhardware mit bestehender Herstellergarantie und definierten Wiederherstellungszeiten (Server, Storage, Tape Library, NAS, Wasabi Cloud Speicher an geografisch anderem Standort)
- Betrieb der Server im Hochverfügbarkeits-Verbund
- Definierte RAID-Level auf Server (RAID5, RAID10) und NAS (RAID5)
- Backup- & Recovery-Konzept mit geografisch getrennter Speicherung (Wasabi)
- Regelmäßige Updates und Sicherheitspatches der eingesetzten Software auf Servern und Firewalls
- Laufende Systemüberwachung und Kapazitätsanalyse, insbesondere in Anbetracht der Spitzenlast
- Bestehendes Notfallkonzept, z.B. für Notstromversorgung, Cyberabwehr, das regelmäßig auf Wirksamkeit geprüft wird

h) Trennungskontrolle:
Allgemein:
- Kundendokumentationen befinden sich in getrennten Ordner- und Bereichsstrukturen
- Trennung von Produktiv- und Testsystemen

Rechenzentrum:
- netzwerkseitige Mandantentrennung über VLAN-Segmentierung, sodass ein Zugriff auf Datenbestände der Kunden untereinander unmöglich ist

Anlage 2 – Art, Zweck und Kreis der Betroffenen der verarbeiteten Kundendaten (Version 2.0 vom 01.03.2022)

Art der Daten	Zweck der Datenverarbeitung	Art der Datenverarbeitung	Kreis betroffener Personen
Personenstamm-, Kommunikations-, Vertragsstammdaten, Kundenhistorie, Abrechnungs- und Zahlungsdaten	- Angebots- und Auftragsabwicklung, Rechnungswesen	Speicherung, Zugriff, Modifizierung, Anpassung oder Änderung, Verschiebung, Beschränkung, Löschung	Mitarbeiter, Kunden, Behörden, Interessenten, Lieferanten
Innerhalb der IT-Dienstleistungen und des Hostings mögliche vorkommende Daten auf Kundensystemen: Personenstammdaten, Vertragsstammdaten, Planungs- und Steuerungsdaten, Kundenhistorie, Gesundheitsdaten Soziale Daten, Biometrische Daten, Finanzdaten, Sonstige Daten	- Hosting und Bereitstellung von IT-Systemen mittels Rechenzentrum - Erbringung von IT-Dienstleistungen und IT-Support	Speicherung, Zugriff, Änderung, Verschiebung, Modifizierung, Anpassung oder Änderung, Updates über Fernwartung, Einsichtnahme, Fehleranalyse und Fehlerbehebung/Übertragung, Weitergabe, Netzwerkeinrichtung / Vernetzung	Mitarbeiter, Kunden, Kunden des Auftraggebers, Behörden
IT-Dokumentation mit Passwörtern (Server, Clients, Software etc.)	- Dokumentationszwecke für laufende IT-Betreuung	Speicherung, Zugriff, Änderung, Verschiebung, Modifizierung, Anpassung oder Änderung, Updates über Fernwartung, Einsichtnahme, Fehleranalyse und Fehlerbehebung/Übertragung, Weitergabe, Netzwerkeinrichtung / Vernetzung	Mitarbeiter, Kunden, Behörden, Interessenten
alle auf Datenträger gespeicherten Daten	- Entsorgung von Festplatten	Löschung	Mitarbeiter, Kunden

Anlage 3 – Auflistung der Subunternehmer (Version 2.0 vom 04.02.2026)

Kategorie des Subunternehmers	Beschreibung der Teilleistungen
3CX GmbH (gehört zur 3CX Ltd.) 4, Markou Drakou, 2409 Engomi, Nicosia, Cyprus	Cloudtelefonie für Sprachkommunikation (intern und mit Kunden, Partnern, Dritten)
ADN – Advanced Digital Network Distribution GmbH Josef-Haumann-Str. 10, 44866 Bochum	Cloud Marketplace zur Bestellung von M365 Services und zur Anlage der Microsoft Tenants
Bitwarden, Inc. 1 North Calle Cesar Chavez, Santa Barbara, CA 93103, USA	Passwortverwaltung für interne Zwecke und Kunden Rechtsgrundlage für den Datentransfer: EU-U.S. Data Privacy Framework
c-entron Software GmbH Einsteinstraße 59, 89077 Ulm	Software für Systemhäuser (ERP, CRM) mit Service-Board (Ticketsystem)
Cisco Systems, Inc. 170 West Tasman Dr., San Jose, CA 95134 USA	Bereitstellung von Duo Security als Lösung für Multifaktor-Authentifizierung Rechtsgrundlage für den Datentransfer: EU-U.S. Data Privacy Framework
DocuSign Germany GmbH Neue Rothofstrasse 13-19, 60313 Frankfurt	Digitaler Austausch von Vertragsdokumenten unter Verwendung einer rechtsgültigen eSignatur
Docusnap GmbH Franz-Larcher-Straße 4, 83088 Kiefersfelden	Bereitstellung von Docusnap (IT-Dokumentationssoftware)
dogado GmbH Antonio-Segni-Straße 11, 44263 Dortmund	Webhosting, Mailhosting, Domainhosting
Elbtal Steuerberatung GmbH Königstraße 17, 01097 Dresden	Finanzbuchhaltung
ELOVADE Deutschland GmbH Garbenheimer Str. 36, 35578 Wetzlar	Bereitstellung EL Storage als S3-kompatiblen Cloud-Speicher für Wasabi Backup, Bezug eset Virenschutz
Fsas Technologies GmbH Mies-van-der-Rohe-Straße 8, 80807 München *und deren autorisierte Servicepartner*	Lieferung von Hard-/Software, Ersatzteile, Garantieabwicklung Client-/Server-/Storagesysteme
Hornetsecurity GmbH Am Listholze 78, 30177 Hannover	Lösungen für den Schutz von Microsoft 365 Diensten inkl. Archivierung und Backup
ITscope GmbH Durlacher Allee 73, 76131 Karlsruhe	Online-Handelsplattform mit Anbindung an c-entron Warenwirtschaft
Lenovo (Deutschland) GmbH Löffelstraße 40, 70597 Stuttgart	Lieferung von Hard-/Software, Ersatzteile, Garantieabwicklung Client-/Server-/Storagesysteme
Microsoft Corporation One Microsoft Way, Redmond, WA 98052-6399, USA	Lieferung von Hard-/Software (Server- und Client-OS), Bereitstellung von Cloud Services (SaaS), z. B. M365 und Azure Rechtsgrundlage für den Datentransfer: EU-U.S. Data Privacy Framework
NinjaOne, LLC 3687 Tampa Rd., Suite 200, Oldsmar FL 34677, USA	Netzwerk-Monitoring für Kundensysteme, Update- und Patchmanagement Rechtsgrundlage für den Datentransfer: EU-U.S. Data Privacy Framework
NorthC Deutschland GmbH Am Tower 5, 90475 Nürnberg	Rechenzentrumsbetreiber, Colocation, Bereitstellung Data Center Environment, Hands-On-Support für Hardware
QualityHosting AG Uferweg 40-42, 63571 Gelnhausen	Hosted Exchange Server, Domainhosting
ratiokontakt GmbH Starkenfeldstraße 21, 96050 Bamberg	Webhosting, Mailhosting, Domainhosting
REISSWOLF Akten- und Datenvernichtung GmbH Fischweg 14a, 09114 Chemnitz	Festplatten- und Datenträgervernichtung, Aktenvernichtung
Sendinblue GmbH Köpenicker Str. 126, 10179 Berlin	Newsletterversand
STRATO AG Pascalstr. 10, 10587 Berlin	Domainhosting
TeamViewer GmbH Jahnstr. 30, 73037 Göppingen	Fernwartungslösung für Remote-Support. Update- und Patchmanagement
TREND MICRO Deutschland GmbH Zeppelinstraße 1, 85399 Hallbergmoos	Malware-Prüfung über die Produkte Cloud App Security, Email Security, Worry-Free Services, Cloud basierte Verwaltung des Virenschutzes
Veeam Software Group GmbH Linden Park, Lindenstrasse 16, CH-6340 Baar, Schweiz	Replikations- und Datensicherungslösungen
Wasabi Technologies LLC 75 Arlington St., Suite 810, Boston, MA 02116, USA	Bereitstellung von Cloud-Backup-Speicher innerhalb Deutschlands Rechtsgrundlage für den Datentransfer: EU-Standardvertragsklauseln
WatchGuard Technologies, Inc. 255 S. King St. Suite 1100, Seattle, WA 98104, USA	Bereitstellung von Firewall Appliances mit Sicherheitsfunktionen und Filtermechanismen, Virenschutz, cloudbasiertes Monitoring, cloudbasierte Verwaltung des Virenschutzes Rechtsgrundlage für den Datentransfer: EU-U.S. Data Privacy Framework