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