Anlage 1 – Technisch-organisatorische Maßnahmen (Version 2.0 vom 01.03.2022)

a) Überblick über die Maßnahmen zur Zutrittskontrolle:
Bürogebäude (Würzburger Straße 14, 01187 Dresden, 5. Etage):
- Sicherheitsschließung zu den Geschäftsräumen von ditpro
- Schlüsselverwaltung zentral nach Protokoll geregelt
- klare Zuweisungen der Berechtigungen (Archiv, Büro, Serverraum)
- Büroräume und Schränke stets verschlossen (Zutritt Externer nur über Anmeldung)
- sorgfältige Auswahl von Reinigungspersonal

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

b) Überblick über die Maßnahmen zur Zugangskontrolle:
- authentifizierter Zugriff auf Systeme des Auftraggebers mittels Fernwartungssoftware TeamViewer: Es sind Kennwortverfahren mit vorgegebener Mindestlänge sowie ein regelmäßiger Wechsel des Kennworts festgelegt
- authentifizierter Zugriff auf IT-Dokumentation des Auftraggebers: Der Datenzugriff erfolgt nur zu Wartungs- und Supportzwecken für berechtigte Administratoren des Auftragnehmers mit unterzeichneter Geheimhaltungsvereinbarung
- personalisierter, authentifizierter Zugang auf die Basisplattform im Rechnenzentrum ausschließlich per ipSec-VPN
- Mitarbeiter-PCs sind kennwortgeschützt mit Vorgabe für Länge und Zeichen der Passwörter
- Anweisung zur Änderung der Standard-Passwörter
- keine Weitergabe der Passwörter
- Automatisches Sperren von PCs bei Inaktivität
- Einsatz von Anti-Viren-Programmen und Firewalls

c) Überblick über die Maßnahmen zur Zugriffskontrolle:
- Administratoren mit Zugriffsberechtigung sind namentlich bekannt, durchgeführte Arbeiten mit Datenzugriff werden über das Helpdesk-System des Auftragnehmers dokumentiert.
- Berechtigungskonzept, Zugriffsrechte sowie deren Überwachung und Protokollierung
- Anzahl der Administratoren auf das „Notwendigste" reduziert
- Verwaltung der Rechte durch Geschäftsführer IT
- Sichere Aufbewahrung von Datenträgern auch am Arbeitsplatz z. B. USB Sticks
- Einsatz von Aktenvernichtern bzw. zertifizierten Dienstleistern
- Ordnungsgemäße Vernichtung von Datenträgern
- Verschlüsselung von Festplatten in Laptops

d) Weitergabekontrolle von Daten:
- ohne Zustimmung keine Weiterleitung von Mails
- kennwortgeschützte Übermittlung von vertraulichen Daten (z.B. Dokumentationen)
- Remotezugriff über eine verschlüsselte Verbindung des Softwareherstellers TeamViewer, RDP oder VPN
- Festplatten-Vernichtung erfolgt nach BDSG und DIN 66399 in der Sicherheitstufe H-4, Schutzklasse 2 (hoher Schutzbedarf, Materialteilchenfläche nach der Vernichtung =< 160mm^2)
- Festplatten-Vernichtung wird mit jeder einzelnen Seriennummer dokumentiert und zertifiziert

e) Eingabekontrolle:
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (teilweise, nicht überall möglich)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts (teilweise, nicht überall möglich)
- durchgeführte Arbeiten mit Datenzugriff werden über das Helpdesk-System des Auftragnehmers dokumentiert
- Änderungen an der Kundendokumentation werden in einer Versionierung erfasst

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

g) Verfügbarkeitskontrolle:
Bürogebäude (Würzburger Straße 14, 01187 Dresden, 5. Etage):
- Offline-Synchronisierung der Kundendaten auf Mitarbeiter-PCs
- Wiederherstellung durch erneute Synchronisierung jederzeit möglich

Rechenzentrum (QSC AG, Am Tower 5, 90475 Nürnberg) als Subunternehmer:
- TÜV-geprüftes Rechenzentrum (ISO 27001:2005, ISO 9001:2008)
- redundante Auslegung der Trafo- und USV-Anlagen
- 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
- Unterbrechungsfreie Stromversorgung (USV)
- Serverräume können nur durch einen bestimmten Personenkreis betreten werden
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen

Rechenzentrum (eigene Rechenzentrumshardware des Auftragnehmers)
- Markenhardware mit bestehender Herstellergarantie und definierten Wiederherstellungszeiten (Server, Storage, Tape Library, NAS)
- Betrieb der Server im Hochverfügbarkeits-Verbund
- Definierte RAID-Level auf Server (RAID5, RAID10) und NAS (RAID5)
- Bestehen eines Backup- & Recoverykonzepts
- Aufbewahrung von Datensicherungen im zweiten Brandabschnitt
- kontinuierliche Einspielung von Updates und Sicherheitspatches der eingesetzten Software auf Servern und Clients

h) Trennungskontrolle:
- IT-Dokumentationen der Auftraggeber befinden sich in getrennten Ordnerstrukturen
- Trennung von Produktiv- und Testsystemen