Technisch-organisatorische Maßnahmen zu Vereinbarung über die Auftragsverarbeitung gemäß Art. 28 DS-GVO

1. Transparenz (Art. 5 Abs. 1 lit. a DSGVO)

☒ Dokumentierung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung
☒ Dokumentation der Empfänger von Daten, sowie der Zeitspanne der Überlassung
☒ Dokumentierung der Mandanten sowie der zugehörigen Datenbereiche
☒ Dokumentierung verbindlicher Löschfristen
☒ Auf Antrag der betroffenen Person: Bereitstellung der hier markierten Dokumentation
☒ Veröffentlichung der Informationen zur Verarbeitung von personenbezogenen Daten als Datenschutzerklärung

2. Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO)

☒ Darstellung der Zwecke im Verzeichnis Verarbeitungstätigkeiten
☒ Verpflichtung der Mitarbeiter die Anforderungen der DSGVO zu beachten
☒ Bestimmung einer schriftlichen Dienstanweisung zur Verarbeitung personenbezogener Daten

3. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

☒ Schlüsselregelung
☒ Zeitliche Zugangsbeschränkung
☒ Benutzerkonto für jeden Mitarbeiter
☒ Passwort Authentifizierung
☒ Authentifikation über Verzeichnisdienste
☒ Aufteilung der Administratorrechte unter verschiedenen Personen
☒ Vergabe der Administratorrechte an eine minimale Anzahl von Personen
☒ Sicheres Löschen von einzelnen Dateien
☒ Differenzierung administrativer Aufgaben
☒ Logische Mandantentrennung
☒ Trennung von Produktiv- und Testsystem
☒ Datenkommunikation über VPN-Tunnel

4. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

☒ Signieren elektronischer Dokumente
☒ Überwachung von Fernwartungsaktivitäten
☒ Einsatz von Virenschutzsoftware
☒ Application Layer Firewall
☒ Packet Filter Firewall
☒ Differenzierte Berechtigungen für unterschiedliche Transaktionen
☒ Differenzierte Berechtigungen für Datenobjekte

5. Verfügbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

☒ Wiederherstellungs- und Sicherungskonzept (Recovery & Backup)
☒ Automatisiertes Anfertigen von Backups (Datensicherungen)
☒ Festgelegte Zuständigkeiten für die Datensicherung
☒ Datenreplikation
☒ Automatisiertes Benachrichtigungssystem bei Ausfall

6. Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

☒ Lastverteilung der Netzwerkkomponenten (load balancing)
☒ Lastverteilung der Server (load balancing)
☒ Lastverteilung der Dienste (load balancing)
☒ Automatische Skalierung virtueller Systeme
☒ Unterbrechungsfreie Stromversorgung
☒ Überspannungsschutz
☒ Rauch- und Feuermeldeanlagen
☒ Einsatz von IT-Systemen welche über die erforderliche Leistungsfähigkeit verfügen
☒ Wassereinbruchschutz
☒ Hochwasserschutz
☒ Automatisches Notrufsystem
☒ Eignung des Baus und der Räumlichkeiten

7. Rechenschaftspflicht und Wirksamkeitsnachweis (Art. 5 Abs. 2 DSGVO/ Art. 32 Abs. 1 lit. d DSGVO)

☒ Führen eines Verzeichnisses von Verarbeitungstätigkeiten
☒ Bestellung einer Datenschutzbeauftragtin bzw. eines Datenschutzbeauftragten
☒ Dokumentierung der vorhandenen IT-Infrastruktur
☒ Dokumentierung eingesetzter Programme und Anwendungen
☒ Protokollierung von Anmeldevorgängen
☒ Protokollierung von Datenzugriffen
☒ Protokollierung gescheiterter Zugriffs versuche
☒ Sicherung der Protokolldaten gegen Veränderung oder Verlust
☒ Automatisierte Auswertung der Protokolldaten
☒ Protokollierung von Löschvorgängen
☒ Protokollierung von Übermittlungsvorgängen
☒ Benutzerkennungsbezogene Protokollierung
☒ Protokollierung aller Administratorenaktivitäten
☒ Protokollierung der Eingabe bei der Erhebung und Ergänzung von Daten
☒ Protokollierung der Veränderung oder Korrektur von gespeicherten Daten