Anlage 2 – technische und organisatorische Maßnahmen

Nachfolgende technische und organisatorische Maßnahmen sind für die im Vertrag genannte Verarbeitung von personenbezogenen Daten durch den Auftragnehmer zur Gewährleistung von Datenschutz und Datensicherheit gem. Art. 32 DSGVO implementiert. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.
Diese Maßnahmen gelten auch für den Standort Hamburg. Bei Abweichung von den TOMs des Hauptstandortes Mettingen sind diese gesondert beschrieben (Kürzel HH).

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

Die Sicherstellung der Vertraulichkeit der Datenverarbeitungssysteme gehört zu den Schlüsselelementen moderner Sicherheitsmechanismen und ist Bestandteil der wesentlichen Schutzziele der DSGVO. Maßnahmen zur Umsetzung des Gebots der Vertraulichkeit sind unter anderem auch solche, die zur Zutritts-, Zugangs- und Zugriffskontrolle gehören. Die in diesem Zusammenhang getroffenen technischen und organisatorischen Maßnahmen sollen eine angemessene Sicherheit der personenbezogenen Daten gewährleisten.

Zutrittskontrolle

Verwehrung des Zutritts für Unbefugte zu Verarbeitungsanlagen:

☒	Alarmanlage (HH: nicht vorhanden)
☒	Automatisches Zugangskontrollsystem (HH: nicht vorhanden)
☐	Schließsystem mit Codesperre
☐	Biometrische Zugangssperren
☐	Lichtschranken / Bewegungsmelder
☒	Manuelles Schließsystem inkl. Schlüsselregelung (nur HH) (keine Schlüsselausgabe)
☐	Protokollierung der Besucher
☐	Sorgfältige Auswahl von Wachpersonal
☒	Chipkarten- / Transponder-Schließsystem (HH: nicht vorhanden)
☒	Videoüberwachung der Zugänge (HH: nicht vorhanden)
☐	Sicherheitsschlösser
☒	Personenkontrolle beim Empfang (Ist der Empfang nicht besetzt, sind alle Türen verschlossen.)
☒	Besucherbegleitung während des gesamten Aufenthalts
☒	Sorgfältige Auswahl von Reinigungspersonal
☐	Tragepflicht von Mitarbeiter-/Gästeausweisen
☒	gesicherter Serverraum (eigene Schließanlage; Schlüsselvergabe nach strengen Kriterien) (HH: kein Server vor Ort; Zugriff auf Server am Hauptstandort über Firewall und VPN)

☒	Clean-Desk-Regelungen

Zugangskontrolle / Benutzerkontrolle

Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte:

☒	Authentifikation mit Benutzername / Passwort
☐	IT-Sicherheitsrichtlinien
☐	Einsatz von Intrustion-Detection-Systemen (IDS)
☒	Einsatz von Anti-Viren-Software
☒	Einsatz einer Hardware-Firewall
☒	Einsatz einer Software-Firewall
☒	Erstellen von Benutzerprofilen
☒	Einsatz von VPN-Technologie
☐	Verschlüsselung von mobilen Datenträgern
☐	Verschlüsselung von Datenträgern in Laptops / Notebooks
☐	Einsatz von zentraler Smartphone-Administrations-Software

Zugriffskontrolle / Datenträgerkontrolle /Speicherkontrolle

Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern, Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten. Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den ihrer Zugangsberechtigung unterliegenden personenbezogenen Daten Zugang haben:

☒	Rolle und Berechtigungen auf Basis „Need to Know Prinzip“
☒	Verwaltung der Rechte durch definierte Systemadministratoren
☒	Anzahl der Administratoren auf das „Notwendigste“ reduziert
☒	Vorgaben zum Remote-Zugang zu den Datenverarbeitungssystemen
☐	Vergabe- und Entzugsprozess von Berechtigungen (Dokumentierte Prozesse bei Einstellung/Ausscheiden von Berechtigten)
☒	Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
☒	physische Löschung von Datenträgern vor Wiederverwendung
☒	Einsatz von Aktenvernichtern u. eines Dienstleisters zur Entsorgung
☒	Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel

☒	Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
☒	Protokollierung der Vernichtung

Trennungsgebot / Trennbarkeit

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Nachfolgende technische und organisatorische Maßnahmen sind für die im Vertrag genannte Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch den Auftragnehmer implementiert:

☐	physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
☒	Versehen der Datensätze mit Zweckattributen/Datenfeldern
☐	Festlegung von Datenbankrechten
☒	Logische Mandantentrennung (softwareseitig)
☐	Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
☒	Trennung von Produktiv- und Testsystem

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

Maßnahmen, die gewährleisten, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen, die eine unbefugte Identifizierung der betroffenen Person ausschließen.

☐	Verwendung von (Personal-, Kunden- oder Patienten-) Kennziffern statt Namen
☐	Verschlüsselung von Zusatzinformationen zur Identifikation
☐	Verwaltung und Dokumentation von differenzierten Berechtigungen auf die Zusatzinformationen zur Identifikation
☐	Autorisierungsprozess oder Genehmigungsroutinen für Berechtigungen zur Verarbeitung von Zusatzinformationen zur Identifikation
☐	Autorisierungsprozess oder Genehmigungsroutinen für Berechtigungen zur Verarbeitung von Zusatzinformationen zur Identifikation
☐	Kopierschutz hinsichtlich Zusatzinformationen zur Identifikation
☐	Vier-Augen-Prinzip für Identifikation

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

Maßnahmen zur Umsetzung des Gebots der Integrität sind solche, die generell zum Schutz vor unbefugter, unrechtmäßiger bzw. unbeabsichtigter Verarbeitung, Zerstörung bzw. Schädigung beitragen.

Weitergabekontrolle / Transportkontrolle

Maßnahmen, die gewährleisten, dass bei der Übermittlung personenbezogener Daten, sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt wird:

☒	Einrichtung von VPN-Tunneln
☒	Verschlüsselte Datenübertragung im Internet (z.B. HTTPS, SFTP, 256-Bit-AES etc.)
☒	E-Mail-Verschlüsselung (bei Bedarf)
☒	Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und –fahrzeugen
☐	Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
☐	Beim physischen Transport: sichere Transportbehälter/-verpackungen

Eingabekontrolle / Übertragungskontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind, sowie, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten übermittelt oder zur Verfügung gestellt wurden oder werden können:

☒	Protokollierung der Eingabe, Änderung und Löschung von Daten
☒	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
☒	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
☐	Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
☒	Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
☒	Protokollierung von Support-Tickets

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

Personenbezogene Daten sind gegen unbefugte, unrechtmäßige, unbeabsichtigte bzw. zufällige Zerstörung oder Verlust zu schützen. Diese Maßnahmen müssen so ausgelegt sein, dass sie die Verfügbarkeit der personenbezogenen Daten auf Dauer gewährleisten.

Zuverlässigkeits- / Datenintegritäts- / Verfügbarkeits- / Wiederherstellungskontrolle

Maßnahmen, die gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und Maßnahmen, die gewährleisten, dass eingesetzte Systeme bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können:

☒	Unterbrechungsfreie Stromversorgung (USV)
☒	Verwendung von RAID-Systemen
☒	Verwendung von Virenschutz und Firewalls
☐	Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
☐	Feuer- und Rauchmeldeanlagen
☐	Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
☒	Testen von Datenwiederherstellung
☒	Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
☐	In Hochwassergebieten: Serverräume über der Wassergrenze
☒	Klimaanlage in Serverräumen
☒	Schutzsteckdosenleisten in Serverräumen
☒	Feuerlöschgeräte
☒	Backup- & Recovery Konzept
☐	Erstellen eines Notfallplans

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

Damit sind Maßnahmen gemeint, um insbesondere die schon getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit laufend aktuell zu halten und kritisch zu begutachten. Diese Pflicht erstreckt sich auf alle technischen und organisatorischen Maßnahmen.

☒	Datenschutz-Management
☒	Risiko-Bewertung
☐	Incident Response Management
☐	Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)
☒	Auftragskontrolle (eindeutige Vertragsgestaltung, strenge Auswahl des Dienstleisters etc.)

5. internes Datenschutz-Management

☒	Richtlinien zum Datenschutz
☒	Richtlinien zur IT-Sicherheit
☒	Risikomanagement
☒	Verpflichtung der Mitarbeiter auf den Datenschutz, das Datengeheimnis und die Vertraulichkeit
☐	Verpflichtende Standards und Richtlinien für das Mobile Arbeiten
☒	Auditplanung und Durchführung von internen- und externen Audits
☒	Schulungen zum Datenschutz und der IT-Sicherheit