**Technische und organisatorische Maßnahmen nach Art. 32 DSGVO**

**mit Stand vom 02.11.2021**

1. **Vertraulichkeit**

a) Zutrittskontrolle

Der Auftragnehmer trifft Maßnahmen, mit denen Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen die personenbezogenen Daten verarbeitet werden. Der Auftragnehmer ergreift in diesem Zusammenhang Maßnahmen, die dafür Sorge tragen, dass nur die Personen Zutritt zu den Anlagen haben, mit denen personenbezogene Daten verarbeitet werden, die über eine entsprechende Berechtigung verfügen. Im Einzelnen werden folgende Maßnahmen durchgeführt:

| Technische Maßnahmen | Organisatorische Maßnahmen |
|---|---|
| ☒ Alarmanlage | ☒ Schlüsselverwaltung |
| ☐ Automatisches Zugangskontrollsystem | ☐ Empfang/ Rezeption/ Pförtner |
| ☐ Biometrische Zugangssperren | ☐ Besucherbuch/ Protokoll der Besucher |
| ☒ Chipkarten/Transpondersysteme | ☐ Mitarbeiter-/Besucherausweise |
| ☒ Manuelles Schließsystem | ☒ Besucher nur in Begleitung durch Mitarbeiter |
| ☒ Sicherheitsschlösser | ☐ Sorgfältige Auswahl von Wachpersonal |
| ☐ Schließsystem mit Codesperre | ☐ Sorgfältige Auswahl von Reinigungsdiensten |
| ☐ Absicherung der Gebäudeschächte | ☒ Verpflichtung von Externen auf Wahrung der Vertraulichkeit |
| ☒ Türen mit Knauf außenseitig | ☐ |
| ☐ Klingelanlage mit Kamera | ☐ |
| ☒ Videoüberwachung der Eingänge | ☐ |
| ☒ Bewegungsmelder | ☐ |
| ☐ | ☐ |
| ☐ | ☐ |

b) Zugangskontrolle

Der Auftragnehmer ergreift Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und -verfahren benutzen. Der Auftragnehmer ergreift in diesem Zusammenhang Maßnahmen, die dafür Sorge tragen, dass nur die Personen auf Anlagen zur Datenverarbeitung zugreifen können, die über eine entsprechende Berechtigung verfügen. Im Einzelnen werden folgende Maßnahmen durchgeführt:

| Technische Maßnahmen | Organisatorische Maßnahmen |
|---|---|
| ☒ Login mit Benutzername und Passwort | ☒ Verwalten von Benutzerberechtigungen |
| ☐ Login mit biometrischen Daten | ☒ Erstellen von Benutzerprofilen |
| ☒ Automatische Desktopsperre, 10 Minuten | ☒ Anzahl der Administratoren beschränkt |
| ☒ Anti-Viren-Software Server | ☒ Zentrale Passwortvergabe |
| ☒ Anti-Viren-Software Clients | ☒ Richtlinie „Sicheres Passwort“ |
| ☒ Anti-Virus-software Mobile Geräte | ☒ Richtlinie „Löschen/ Vernichten“ |
| ☒ Einsatz von Hardware-Firewall | ☐ Richtlinie „Clean desk“ |
| ☒ Einsatz von Software-Firewall | ☒ Sichere Aufbewahrung von Datenträgern |
| ☐ Intrusion Detection Systeme | ☒ Allg. Richtlinie Datenschutz und/ oder Sicherheit |
| ☐ Intrusion Pervention Systeme | ☒ Mobile Device Policy |
| ☒ Mobile Device Management | ☐ Anleitung „Manuelle Desktopsperre“ |
| ☒ Einsatz VPN bei Remote-Zugriffen | ☒ Verbot zur Nutzung von privaten Speichermedien |

| | |
|---|---|
| ☒ Verschlüsselung von Datenträgern | ☒ Konzept zum Umgang mit Daten an Telearbeitsplätzen/ Heimarbeit vorhanden |
| ☒ Verschlüsselung von Smartphones | ☐ Keine Speicherung von Zugangsdaten beim Login |
| ☐ Sperre externer Schnittstellen (USB) | ☐ |
| ☒ Festplattenverschlüsselung von Notebooks | |

c) Zugriffskontrolle

Damit sind Maßnahmen gemeint, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können. Der Auftragnehmer ergreift in diesem Zusammenhang Maßnahmen, die dafür Sorge tragen, dass Personen im Rahmen der Datenverarbeitung nur auf die Daten zugreifen können, für die sie über eine entsprechende Berechtigung verfügen und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Im Einzelnen werden folgende Maßnahmen durchgeführt:

| Technische Maßnahmen | Organisatorische Maßnahmen |
|---|---|
| ☒ Physische Löschung von Datenträgern | ☒ Einsatz von Berechtigungskonzepten |
| ☒ Nutzung von Aktenschredder | ☒ Verwaltung der Benutzerrechte durch Administratoren |
| ☒ Protokollierung von Zugriffen | ☒ Sorgfältige Auswahl von externen Datenvernichtern |
| ☒ Protokollierung von Eingaben, Änderungen und Löschung von Daten | ☒ Konzept „Vernichtung von Daten“ |
| ☐ | ☐ Konzept zum Ausscheiden von Mitarbeitern vorhanden (Entzug der Berechtigungen) |
| ☐ | ☐ |
| ☐ | ☐ |
| ☐ | ☐ |
| ☐ | ☐ |

**d) Trennungskontrolle Trennungsgebot**

Damit sind Maßnahmen gemeint, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Der Auftragnehmer ergreift in diesem Zusammenhang Maßnahmen, die dafür Sorge tragen, dass personenbezogene Daten entsprechend den oben genannten Anforderungen getrennt verarbeitet werden. Im Einzelnen werden folgende Maßnahmen durchgeführt:

| Technische Maßnahmen | Organisatorische Maßnahmen |
|---|---|
| ☒ Trennung von Produktiv- und Testumgebung | ☒ Steuerung über Berechtigungskonzept |
| ☒ Physikalische Trennung (Systeme/ Datenbanken/ Datenträger) | ☒ Festlegung von Datenbankrechten |
| ☒ Mandantenfähigkeit relevanter Anwendungen | ☒ Datensätze sind mit Zweckattributen versehen |
| ☐ | ☐ |
| ☐ | ☐ |
| ☐ | ☐ |

| | |
|---|---|
| ☐ | ☐ |

e) Pseudonymisierung & Verschlüsselung

| Technische Maßnahmen | Organisatorische Maßnahmen |
|---|---|
| ☐ Trennung der Zuordnungsdaten und Aufbewahrung in getrennten und abgesicherten Systemen | ☐ Interne Anweisung, p.b. Daten im Falle einer Weitergabe nach Möglichkeit zu anonymisieren/ pseudonymisieren |
| ☐ | ☐ Einschreibung in offenen Aushängen per Mitarbeiter-/ Patienten-ID |
| ☐ | ☐ |
| ☐ | ☐ |
| ☐ | ☐ |

**2. Integrität**

a) Eingabekontrolle

Damit sind Maßnahmen gemeint, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind. Der Auftragnehmer ergreift in diesem Zusammenhang Maßnahmen, die dafür Sorge tragen, dass im Nachhinein überprüft und festgestellt werden kann, ob und durch wen personenbezogene Daten in Datenverarbeitungssysteme des Unternehmens eingegeben, verändert oder entfernt worden sind. Im Einzelnen werden folgende Maßnahmen durchgeführt:

| Technische Maßnahmen | Organisatorische Maßnahmen |
|---|---|
| ☒ Technische Protokollierung der Eingabe, Änderung, Löschung von Daten | ☒ Nachvollziehbarkeit von Eingabe, Änderung, Löschung von Daten durch Individuelle Benutzernamen |
| ☒ Manuelle oder automatisierte Auswertung der Protokolle | ☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung nach Berechtigungskonzept |
| ☒ Nutzung von Digitalen Zeitstempeln und Mitarbeiter ID beim Scannen/ Archivieren | ☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitung übernommen wurden |
| ☒ Versionierung von Dokumenten | ☒ Klare Zuständigkeiten für Löschungen |
| ☐ Nutzung von Thin Clients | ☐ Anweisung das Daten nicht auf dem Desktop gespeichert werden dürfen |
| ☐ | ☐ |
| ☐ | ☐ |
| ☐ | ☐ |

b) Weitergabekontrolle

Damit sind Maßnahmen gemeint, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Der Auftragnehmer ergreift in diesem Zusammenhang Maßnahmen, die dafür Sorge tragen, dass personenbezogene Daten entsprechend den oben genannten Anforderungen geschützt sind. Im Einzelnen werden folgende Maßnahmen durchgeführt:

| Technische Maßnahmen | Organisatorische Maßnahmen |
|---|---|
| ☒ Email-Verschlüsselung | ☒ Dokumentation der Datenempfänger |

| | |
|---|---|
| ☒ Einsatz von VPN | ☒ Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen |
| ☒ Protokollierung der Zugriffe und Abrufe | ☐ Weitergabe in anonymisierter oder pseudonymisierter Form |
| ☐ Sichere Transportbehälter | ☒Protokollierte Übergabe beim Transport von Daten |
| ☒ Bereitstellung über verschlüsselte Verbindungen wie sftp, https | ☐ |
| ☒ Nutzung von Signaturverfahren | ☐ |
| ☐ | ☐ |
| ☐ | ☐ |
| ☐ | ☐ |

### 3. Verfügbarkeit und Belastbarkeit

**Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust. Und rasche Wiederherstellbarkeit von Daten:**

| Technische Maßnahmen | Organisatorische Maßnahmen |
|---|---|
| ☒ Feuer und Rauchmeldeanlagen | ☒ Backup- und Recovery- Konzept ausformuliert |
| ☒ Feuerlöscher ($CO^2$) Serverraum | ☒ Kontrolle des Sicherungsvorgangs |
| ☒ Serverüberwachung Temperatur und Feuchtigkeit | ☒ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse |
| ☒ Serverraum klimatisiert | ☒ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums |
| ☒ USV | ☒ Aufbewahrung der Sicherungsmedien an einem sicheren Ort in einem anderen Brandabschnitt |
| ☒ Schutzsteckdosenleiste Serverraum | ☒ Keine Wasserleitungen/ Sanitäre Einrichtungen im oder oberhalb des Serverraum |
| ☐ Datenschutztresor mit Quelldichtung | ☒ Existenz eines Notfallplan |
| ☒ RAID System / Festplattenspiegelung | ☒ Getrennte Partitionen für Betriebssysteme und Daten |
| ☒ Videoüberwachung Serverraum | ☐ |
| ☐ Bewegungsmelder Serverraum | ☐ |
| ☐ Alarmmeldung bei unberechtigtem Zutritt zum Serverraum | ☐ |
| ☐ | ☐ |
| ☐ | ☐ |
| ☐ | ☐ |

### 4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

a) Datenschutz-Management

| Technische Maßnahmen | Organisatorische Maßnahmen |
|---|---|
| ☐ Software-Lösungen für Datenschutz-Management | ☒ Externer Datenschutzbeauftragter<br><br>Nadine Stolz, Sicherheitstechnik Stolz<br>Konrad-Zuse-Str. 19-21, 36251 Bad Hersfeld |
| ☐ Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeiten für Mitarbeiter | ☒Mitarbeiter geschult und auf Vertraulichkeit/ Datengeheimnis verpflichtet |
| ☐ Sicherheitskonzept nach ISO 27001, BSI IT-Grundschutz oder ISIS12 | ☒ Regelmäßige Sensibilisierung der Mitarbeiter (nachweislich) |
| ☒ Anderweitig dokumentiertes Sicherheitskonzept | ☒ Interner Informationssicherheitsbeauftragter |

| | |
|---|---|
| | Daniel Schröder |
| ☒ Regelmäßige Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen | ☒ Durchführung von Datenschutzfolgeabschätzung bei Bedarf |
| ☐ | ☒ Informationspflicht nach Art. 13 DSGVO ist etabliert |
| ☐ | ☒ Konzept bei Datenpannen vorhanden |
| ☐ | ☒ Im Prozess bei Datenpannen etablierter Vorgang zur Meldung von Datenpannen bei der Aufsichtsbehörde |
| ☐ | ☒ Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden |
| ☐ | ☐ |

b) Datenschutzfreundliche Voreinstellungen

| Technische Maßnahmen | Organisatorische Maßnahmen |
|---|---|
| ☒ Zweckbindung der erhobenen Daten | ☒ Einfache Ausübung des Widerrufsrechts der Betroffenen |
| ☒ Datenminimierung der erhobenen Daten | ☐ |
| ☐ | ☐ |
| ☐ | ☐ |

c) Auftragskontrolle

Damit sind Maßnahmen gemeint, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Im Einzelnen werden folgende Maßnahmen durchgeführt:

| Technische Maßnahmen | Organisatorische Maßnahmen |
|---|---|
| ☐ | ☒Vorherige Prüfung der vom Auftragnehmer getroffenen Schutzmaßnahmen und Dokumentation |
| ☐ | ☒ Sorgfältige Auswahl von Auftragnehmern |
| ☐ | ☒ Bei Bedarf Abschluss von Auftragsverarbeitungsverträgen |
| ☐ | ☒ Schriftliche Weisungen an den Auftragnehmer |
| ☐ | ☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf Vertraulichkeit/ Datengeheimnis |
| ☐ | ☒Verpflichtung zur Bestellung eines DSB bei Auftragnehmer |
| ☐ | ☒ Vereinbarung wirksamer Kontrollrechte beim Auftragnehmer |
| ☐ | ☒ Regelungen zum Einsatz von Subunternehmern |
| ☐ | ☒ Sicherstellung der Vernichtung von Daten nach Beendigung der Tätigkeit |
| ☐ | ☐ |