Technische & organisatorische Maßnahmen

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

1.1 Zutrittskontrolle: Kein unbefugter Zutritt zu Datenverarbeitungsanlagen

- Allgemeiner Perimeterschutz: Empfangsdienst, Zutrittskontrollmaßnahmen an allen möglichen Seiteneingängen
- Türsicherung, z.B. elektronische Türöffner/-schließer, Türknaufe an Notausgangstüren, Panikschlösser und Obentürschließer
- Manuelles Schließsystem, Sicherheitsschlösser (Hauseingänge), Schlüsselverwaltung (Schlüsselausgabe mit Schlüsselbuch, Schlüsselentzug etc.)
- Elektronisches Schließsystem (mit Transponder-Schließsystem)
- Automatische Türprotokollierung
- Geregelte Zutrittsberechtigungsvergabe (Schutzzone Serverraum, Registrierung, Identifikationsregelung Transponder)
- Geschlossene Außen- und Bürotüren und Fenster außerhalb der Betriebszeiten
- Sichtschutzfolien, Serverräume alle ohne Fenster, Einbruchsicherung
- Melder (Temperatur, Rauch, Ausfall Klimatisierung im Hauptserverraum)
- Besucherregelung (Anmeldung bei Verwaltung, Begleitung im Unternehmen, Kontrolle Fremder durch Beschäftigte)
- Arbeitshinweise (Zutrittskontrolle, z.B. Meldepflicht bei Verlust Transponder, Auffälligkeiten)

1.2 Zugangskontrolle: Keine unbefugte Systembenutzung

- Gesicherte Aufstellung aktiver Netzkomponenten
- Server- und Dateisysteme in geschützten Räumlichkeiten
- Gehäuseverriegelungen (Racks Serverräume), Kensington-Schloss (Messegeräte)
- Arbeitshinweise, z. B. Nutzungsverbot nicht freigegebener Hard-/Software (Whitelist, Softwarecenter)
- Einsatz von Anti-Viren-Software; Hardware-/Software-Firewall, Spam-/Content-Filter
- Benutzerverwaltung personenbezogen, Authentifikation mit Benutzer-ID/Passwort
- Abgesicherte Übertragungswege für personenbezogene Daten, z.B. E-Mail-Anhang-/Datenträger-Verschlüsselung, Einsatz von VPN-Technologie, Citrix
- Sichere Aufbewahrung sensibler dienstlicher Unterlagen und Datenträger, z.B. Archivierung
- Sichere Verwahrung und strikt geregelte Nutzung zentraler Schließmedien (Zentralschlüssel)
- Regelmäßige Maßnahmen zur Personalsensibilisierung
- Stichprobenkontrollen zur Einhaltung der Sicherheits-Vorgaben

1.3 Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems

- Funktionelle Zuordnung von Endgeräten
- Verwaltung der Rechte durch Systemadministrator
- Dokumentation der zugelassenen Benutzer und Rechteprofile, Zugriffsmatrix
- Zeitbasierte Zugriffsbeschränkungen (Time-Out)
- Login-Protokollierung, Kontosperre bei Zugangs-Fehlversuchen (z.B. Accounts)
- Geregelte Deaktivierung und Löschung ungenutzter/stillgelegter Konten
- Verschlüsselung von Daten und/oder E-Mail-Anhängen
- Geregeltes Entsorgungskonzept

- Bei besonders schützenswerten Belangen bei Bedarf Einsatz im 4-Augen-Prinzip
- Schutzschränke für sensible Daten und Systeme
- Stichprobenkontrollen zur Einhaltung der Sicherheits-Vorgaben
- Administratoren-Richtlinie (Policy), Aufgabenteilung Admins
- Maßnahmen zur aktiven Verhinderung des Erlangens von Administratorenrechten, z.B. Änderung systemseitiger Standardpasswörter nach Installation
- Regelmäßige Maßnahmen zur Personalsensibilisierung

1.4 Trennungskontrolle: Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden
- Strukturierte Datenhaltung
- Dezidiertes Berechtigungskonzepts für interdisziplinären Zugriff
- Versehen der Datensätze mit Zweckattributen/Datenfeldern/Flags
- Logische Mandantentrennung (softwareseitig)
- Physikalisch getrennte Speicherung, ggf. auf gesonderten Systemen oder Datenträgern
- Ein Dienst pro Server (Web, Mail, File etc.)
- Trennung von Produktiv- und Testsystem

1.5 Pseudonymisierung: Die Verarbeitung personenbezogener Daten so, dass diese ohne zusätzliche Informationen nicht mehr einer betroffenen Person zugeordnet werden können
- Listen ohne Personenbezug (Anonymisierung)
- Ersetzung von Namen etc. durch Pseudonyme, z.B. Kürzel
- Usertracking-Anwendungen ausschließlich Pseudonymisierung

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

2.1 Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport
- Nutzung anonymisierter bzw. pseudonymisierter Daten (Datenvermeidung)
- Authentifizierung des Daten-/Informationsempfängers (organisatorisch und/oder technisch)
- E-Mail-/Leitungs-Verschlüsselung je nach Übermittlungsweg
- Nutzung von Standleitungen bzw. VPN-Tunneln
- Protokollierung der Übermittlung bzw. des gesamten Transportverfahrens (Übergabeprotokoll, Inventarliste bei Übergabe zu vernichtender Hardware)
- Absicherung Transportbehälter/-verpackungen/-Fahrzeuge (bei physischen Transporten)
- Sorgfältige Auswahl und vertragliche Verpflichtung von Geschäftspartner
- Datenschutzkonforme Vernichtung alter oder defekter Datenträger
- Personalsensibilisierung, entsprechende Arbeitsanweisungen (Informations- und Kommunikations-Mitarbeiter etc.)
- Stichprobenkontrollen zur Einhaltung der Sicherheits-Vorgaben

2.2 Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis des bestehenden Berechtigungskonzepts (nur bereichsspezifische Zusatzberechtigungen)
- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Protokollierung der Aktivitäten für die Systemadministration (Zeitpunkt der Aktivität, Angabe des ausführenden Mitarbeiters etc.)

- Stichprobenkontrollen zur Einhaltung der Sicherheitsvorgaben (Protokollauswertungsroutinen etc.)
- Aufbewahrung von Formularen mit Daten, die in automatisierte Verarbeitungen übernommen worden sind (revisionssicher)
- Sorgfältige Einarbeitung der betreffenden Beschäftigten in den ordnungsgemäßen Gebrauch der Systeme und Verfahren, Bereithalten von Handbüchern
- Awareness-Maßnahmen, Personalsensibilisierung, Arbeitsanweisungen

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

3.1 Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust & rasche Wiederherstellbarkeit

- Regelung zum Verfahren bei Daten-/Datenträger-Verlust
- Einbruch-/Diebstahlschutz
- Unterbrechungsfreie Stromversorgung (USV)
- Klimaanlage in Serverräumen
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Schutzsteckdosenleisten in Serverräumen, Überspannungsschutz, getrennt abgesicherte Zweitsicherung für Serverräume
- Brandschutz, Feuer-/Rauchmeldeanlagen, Alarmgeber, z.B. unberechtigter Zutritt, Fernanzeige von Störungen
- Notfallplan
- Backup- & Recovery-Konzept, RAID-System, Testen von Datenwiederherstellung
- Tests neuer Hard-/Software, Tests vor vollständiger Migration
- Redundanz in der technischen und personellen Infrastruktur
- Geordnete Verfahren und Abläufe für Sicherheits-Patches und gemeldete Schwachstellen
- Liste aller Informations- und Kommunikations-Administratoren inkl. Zuständigkeiten und Befugnisse
- Bereichsspezifische Qualifizierungs- und Awareness-Maßnahmen für Informations- und Kommunikations-Mitarbeiter
- Anweisung für den Umgang mit den technischen/automatisierten Systemen
- Dokumentation Infrastruktur, datenverarbeitenden Systeme und Prozesse (Netzpläne etc.)
- Systemkennzeichnung
- Hard- und Software-Inventarisierung, Lizenzverwaltung/Versionskontrolle Standardsoftware
- Auswahl von kompatiblen Systemen, Komponenten und Telekommunikations-Endgeräten/PDAs
- Schutz von Internetdateien und Systemen (Website, Formulare, PCI-DSS)
- Dateinamenskonvention, Wahl geeigneter Datenformate

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

4.1 Datenschutz-Management

- Durchgängige Datenschutzorganisation
- Etablierter DSB mit Stellvertretern
- Fortlaufende Beratung bei geplanten bzw. zu ändernden Verfahrensweisen
- Regelmäßige Datenschutzaudits (Messung des gelebten Datenschutzniveaus)
- Regelmäßige Berichte an die Geschäftsführung
- Kontinuierliche Personalsensibilisierung

- Begehungen
- Umsetzungskontrollen
- Etablierte Verfahren zu gängigen Datenschutzaufgaben
- Einbindung des Datenschutzes in das Qualitätsmanagement

4.2 Incident-Response-Management
- Verfahren zur Meldung möglicher Datenschutzlücken
- Verfahren zur Meldung von Datenschutzvorfällen

4.3 Auftragskontrolle
- Zentrales Vertragsmanagement
- Sorgfältige Auswahl von Auftragsverarbeitern
- Vereinbarung zur Auftragsverarbeitung
- Kontrollen nach Abschluss der Vereinbarung

4.4 Datenschutzfreundliche Voreinstellungen
- Gemäß Produkt-Datenschutzkonzept

4.5 Datenschutzfreundliches Produktdesign
- Gemäß Produkt-Datenschutzkonzept

Die jeweils aktuelle Fassung unserer Technischen und Organisatorischen Maßnahmen steht unter https://thieme-compliance.de/datenschutz zur Verfügung.