**Übersicht über die Technisch-Organisatorischen Maßnahmen   
(im Weiteren TOM´s) der Praxis nach Artikel 32 EU-Datenschutz-Gesetzverordnung (im Weiteren DSGVO)**

**Die nachfolgenden technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften dienen, sind in der Praxis vorhanden\*:**

|  |
| --- |
| **A) Vertraulichkeit** |

**1. Zutrittskontrolle**

Maßnahmen, mit denen Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird

|  |  |  |  |
| --- | --- | --- | --- |
|  | Es existieren folgende Maßnahmen zur Zutrittskontrolle: | | |
|  | Alarmanlage |  | Videoüberwachung |
|  | Schlüsselregelung (Schlüsselausgabe etc.) |  | Sicherheitsschlösser |
|  | Absicherung von Gebäudeschächten |  | Sorgfältige Auswahl der Mitarbeiter |
|  | Manuelles Schließsystem |  | Sorgfältige Auswahl von Reinigungspersonal, Wachpersonal und Externen, denen Zutritt zu der Praxis gewährt werden muss |

**2. Zugangskontrolle**

Maßnahmen, mit denen die Nutzung von Datenverarbeitungssystemen durch Unbefugte verhindert wird:

|  |  |  |  |
| --- | --- | --- | --- |
|  | Es existieren folgende Maßnahmen zur Zugangskontrolle: | | |
|  | Zuordnung von Benutzerrechten |  | Erstellen von Benutzerprofilen |
|  | sichere, starke Passwortvergabe |  | getrennter Anmelde- und Empfangsbereich vom Wartezimmer |
|  | Authentifikation mit Benutzername/Passwort |  | Verschlüsselung von mobilen Datenträgern |
|  | Gehäuseverriegelungen |  | Einsatz von VPN-Technologie |
|  | Sperren von externen Schnittstellen (USB etc.) |  | Sicherheitsschlösser |
|  | Schlüsselregelung (Schlüsselausgabe etc.) |  | Einsatz von Anti-Viren-Software |
|  | eingerichtete Bildschirmsperren |  | verschließbare Karteischränke |
|  | Für Patienten und Externe unzugänglicher Aufbewahrungsort von PC und Fax |  | Verschlüsselung von Datenträgern in Laptops/Notebooks |
|  | Kontinuierliche Besetzung des Anmelde- und Empfangsbereiches |  | Zuordnung von Benutzerprofilen zu IT-Systemen |
|  | sorgfältige Auswahl von Reinigungspersonal und Wartungsdienstleistern |  |  |

**3. Zugriffskontrolle**

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugangsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt, gelesen, kopiert, verändert oder entfernt werden können:

|  |  |  |  |
| --- | --- | --- | --- |
|  | Es existieren folgende Maßnahmen zur Zugriffskontrolle: | | |
|  | Erstellen eines Berechtigungskonzepts |  | Verwaltung der Rechte durch Systemadministrator |
|  | Anzahl der Administratoren auf das „Notwendigste“ reduziert |  | Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel |
|  | Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten |  | Sichere Aufbewahrung von Datenträgern |
|  | Physische Löschung von Datenträgern vor Wiederverwendung |  | Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399, Schutzklasse 3, Sicherheitsstufe 4 oder 5) |
|  | Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel) |  | Protokollierung der Vernichtung |
|  | Verschlüsselung von Datenträgern |  |  |

|  |
| --- |
| **B) Integrität** |

**1. Weitergabekontrolle**

Maßnahmen, 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:

|  |  |  |  |
| --- | --- | --- | --- |
|  | Es existieren folgende Maßnahmen zur Weitergabekontrolle: | | |
|  | Einrichtungen von Standleitungen bzw. VPN-Tunneln |  | Weitergabe von Daten in anonymisierter oder pseudonymisierter Form |
|  | E-Mail-Verschlüsselung |  | Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen |
|  | Nutzung des SNK |  | Beim physischen Transport: Sichere Transportbehälter/-verpackungen |

**2. Eingabekontrolle**

Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt werden können:

|  |  |  |  |
| --- | --- | --- | --- |
|  | Es existieren keine Maßnahmen zur Eingabekontrolle, weil: | | |
|  | Protokollierung der Eingabe, Änderung und Löschung von Daten |  | Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind |
|  | 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 |  |  |

**3. Auftragskontrolle**

Dabei handelt es sich um Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Der Auftraggeber hat den Auftragnehmer unter den folgenden Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit) auszuwählen und zu beauftragen:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | Es existieren folgende Maßnahmen zur Auftragskontrolle: | | | |
|  | | Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten |  | Vorherige Prüfung und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen | |
|  | | Schriftliche Weisungen an den Auftragnehmer (z. B. durch Auftragsdatenverarbeitungsvertrag)  i.S.d. § 62 BDSG |  | Verpflichtung der Mitarbeiter des  Auftragnehmers auf das Datengeheimnis  (§ 53 BDSG) | |
|  | | Auftragnehmer hat Datenschutzbeauftragten bestellt |  | Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags | |
|  | | Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart |  | Vertragsstrafen bei Verstößen | |
| **C) Verfügbarkeit / Belastbarkeit** | | | |

**1. Verfügbarkeitskontrolle**

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

|  |  |  |  |
| --- | --- | --- | --- |
|  | Es existieren folgende Maßnahmen zur Verfügbarkeitskontrolle: | | |
|  | Unterbrechungsfreie Stromversorgung (USV) |  | Erstellen eines Notfallplans |
|  | Feuer- und Rauchmeldeanlagen |  | Schutzsteckdosenleisten in Serverräumen |
|  | Testen von Datenwiederherstellung |  | Feuerlöschgeräte in Serverräumen |
|  | Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort |  | Erstellen eines Backup- & Recoverykonzepts |

**2. Trennungskontrolle**

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Es existieren folgende Maßnahmen zur Trennungskontrolle: | | |
|  | Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern |  | Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System |
|  | Erstellung eines Berechtigungskonzepts |  | Logische Patiententrennung (softwareseitig) |
|  | Versehen der Datensätze mit Zweckattributen/Datenfeldern |  | Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden |
|  | Festlegung von Datenbankrechten |  | Trennung von Produktiv- und Testsystem |

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Ort, Datum Verantwortlicher

**Diese Übersicht wurde den Mitarbeiterinnen/Mitarbeitern der Praxis am ……………. erläutert und zur Kenntnis gegeben.**

**\*Hinweis:** Aus den gekennzeichneten Bereichen sollten jeweils mindestens zwei Maßnahmen angegeben werden.