[Bearbeitungshinweis:

Bitte lesen Sie diesen Bearbeitungshinweis, bevor Sie die TOMs für Ihre Praxis erstellen.

Neben rechtfertigenden Grundlagen bedarf Datenschutz auch einer realen Form der Datensicherheit. Diese wird durch so genannte TOMs (= technische und organisatorische Maßnahmen) realisiert. Damit sind alle Maßnahmen, die der Datensicherheit und der Schaffung eines angemessenen Datenschutzniveaus dienen, gemeint.

Unter technischen Maßnahmen sind alle verkörperten Maßnahmen der Datensicherheit zu verstehen. Dies können z.B. Aktenvernichter, Datenträger zur Datensicherung, Stahlschränke, Fensterschlösser, Schließanlagen, Überwachungskameras, Feuerlöscher aber auch Passwörter etc. sein.

Organisatorische Maßnahmen sind insbesondere Dienstanweisungen an Mitarbeiter/innen, die den Umgang mit personenbezogenen Daten regeln. Eine typische Dienstanweisung in Ihrer Praxis könnte darin bestehen, dass Patientengespräch nur in Behandlungsräumen mit verschlossener Tür zu führen sind (Diskretion) oder Rezepte nicht offen herumliegen dürfen.

In der Wahl der Mittel sind Sie weitestgehend frei. Sie müssen jedoch beachten, dass alle Sicherheitsmaßnahmen dem aktuellen Stand der Technik entsprechen müssen.

Die TOMs werden in sieben Kategorien eingeteilt. Diese sind:

* Zutrittskontrolle
* Zugangskontrolle
* Zugriffskontrolle
* Weitergabekontrolle
* Eingabekontrolle
* Auftragskontrolle
* Verfügbarkeitskontrolle

Zur Erstellung der TOMs für Ihre Praxis sollten Sie alle sieben Stufen der Reihe nach durchgehen. Dabei ist es normal, wenn Sie bei einigen Kategorien (z.B. Zutrittskontrolle) deutlich mehr Maßnahmen ausweisen können, als bei anderen (z.B. Weitergabekontrolle). Hilfe beim Ausfüllen der einzelnen Stufen sowie Anregungen für einzelne TOMs, die Sie in Ihrer Praxis umsetzen können, finden Sie auf S. 86 – S. 95 unseres Handbuchs „Datenschutz in der Praxis“, das Sie bereits von uns erhalten haben.

Sollten Sie dennoch Fragen haben, zögern Sie bitte nicht, sich an uns zu wenden.

DATA*privat* GmbH

horbach@dataprivat.de

0241-99 77 6 88 3

Entfernen Sie ganz zum Schluss bitte auch diesen Bearbeitungshinweis]

Ihr DATA*privat* Team]

|  |
| --- |
| **1. Zutrittskontrolle** |
| Der Datenschutz beginnt bereits auf der physischen Ebene. Der Verantwortliche hat durch angemessene technische und organisatorische Maßnahmen dafür zu sorgen, dass Unbefugten bereits der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird. |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
|  |
|  |
|  |

|  |
| --- |
| **2. Zugangskontrolle** |
| Die Datenverarbeitungssysteme und Anlagen müssen so beschaffen sein, dass nur diejenigen Personen sie nutzen können, die dazu befugt sind. |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
|  |
|  |
|  |

|  |
| --- |
| **3. Zugriffskontrolle** |
| Es muss gewährleistet sein, dass die zur Benutzung von Datenverarbeitungsanlagen berechtigten Nutzer ausschließlich auf Inhalte zugreifen können, für welche sie berechtigt sind und dass personenbezogene Daten bei der Verarbeitung und Nutzung und nach dem Speichern nicht unbefugt kopiert, verändert oder gelöscht werden können. |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
|  |
|  |
|  |

|  |
| --- |
| **4. Weitergabekontrolle** |
| Es muss verhindert werden, dass personenbezogenen Daten bei der elektronischen Übertragung oder beim Transport oder bei der Speicherung auf Datenträgern unbefugt gelesen, kopiert, verändert oder gelöscht werden können und das festgestellt werden kann, an welchen Stellen eine Übermittlung solcher Daten im Datenverarbeitungssystem vorgesehen ist. |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
|  |
|  |
|  |

|  |
| --- |
| **5. Eingabekontrolle** |
| Im Rahmen der Eingabekontrolle soll die nachträgliche Überprüfbarkeit und Feststellung gewährleistet werden, ob und von wem personenbezogene Daten in Dateiverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
|  |
|  |
|  |

|  |
| --- |
| **6. Auftragskontrolle** |
| Die Verantwortlichen müssen gewährleisten können, dass alle Stellen, welche personenbezogene Daten im Auftrag verarbeiten (Auftragsdatenverarbeitung), ausreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen auch auf deren Seite im Einklang mit der Datenschutz-Grundverordnung bestehen.Bitte geben Sie hier an, wer alles Zugriff auf Patientendaten in Ihrer Praxis hat (außer Angehörige der Praxis selbst oder Ärzte und Steuerberater). |

|  |
| --- |
| Auftragsverarbeiter: |
| **1.** | Name: |
| Anschrift: |
| Telefonnummer: |
| E-Mail-Adresse: |
| (ggf. Internetseite) |

|  |
| --- |
| Auftragsverarbeiter: |
| **2.** | Name: |
| Anschrift: |
| Telefonnummer: |
| E-Mail-Adresse: |
| (ggf. Internetseite) |

|  |
| --- |
| Auftragsverarbeiter: |
| **3.** | Name: |
| Anschrift: |
| Telefonnummer: |
| E-Mail-Adresse: |
| (ggf. Internetseite) |

|  |
| --- |
| **7. Verfügbarkeitskontrolle** |
| Die oder der Verantwortliche muss sicherstellen können, dass sämtliche personenbezogenen Daten, gegen zufällige Zerstörung oder Verlust geschützt sind. Hierzu gehören technische Maßnahmen zum Beispiel am Gebäude und auch EDV-Maßnahmen. |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
|  |
|  |
|  |