Muster

**Aufstellung der Maßnahmen zum Datenschutz („Datenschutzplan für die Arztpraxis“)**

Dieses Muster soll als Orientierungshilfe dienen. Es ist je nach den Umständen des konkreten Einzelfalls anzupassen. Gegebenenfalls können einzelne Aspekte der getroffenen technisch-organisatorischen Maßnahmen (Nr. 1-22) ausgeklammert oder zusammengefasst werden.

**Haftungshinweis:** Das nachstehende Muster ist entsprechend typischen Anforderungen von Praxen und möglichst verständlich formuliert worden. Jedoch sollten Sie das Muster nur nach sorgfältiger Prüfung und Anpassung auf Ihren eigenen Betrieb verwenden. Die Verwendung dieses Musters geschieht auf eigene Verantwortung des Nutzers.

**Urheberrecht:** Sie sind berechtigt, dieses Muster für eigene Zwecke oder innerhalb Ihres Unternehmens auf beliebig vielen Einzelplätzen einsetzen sowie beliebige Anpassungen vorzunehmen. Eine Weitergabe an Dritte (auch an eigene Kunden) ist nur im Rahmen von Mengenlizenzen zulässig.

Muster

**Aufstellung der Maßnahmen zum Datenschutz („Datenschutzplan für die Arztpraxis“)**

**1. Vertraulichkeit und Diskretion**

(Maßnahmen, die verhindern, dass Unbefugte Gespräche in der Praxis mithören. Z.B.: Anmeldebereich ist vom Wartebereich räumlich getrennt. Arzt-Patienten-Gespräche finde in geschlossenen Räumen statt.)

* ..................................
* ..................................

**2. Zugangskontrolle**

(Maßnahmen, die verhindern, dass Unbefugten die Behandlungsräume und die Datenverarbeitungsanlagen zugänglich sind. Z.B.: Türen zu den Praxisräumen sind verschließbar, die Angestellten sind durch Betriebskleidung identifizierbar, die Anmeldung ist während der Sprechzeiten dauerhaft besetzt.)

* ..................................
* ..................................

**3. Gute IT-Strukturen**

(Die Praxis orientiert sich bei der Ausgestaltung der IT-Strukturen an den technischen Anlagen der „Empfehlungen zur Schweigepflicht von KBV und Bundesärztekammer“. Es werden Regelungen zur Datensicherung festgelegt. Z.B: Daten werden täglich gesichert. Kopie wird außerhalb der Praxis aufbewahrt.)

* ..................................
* ..................................

**4. Zugriff auf die Computer**

(Maßnahmen, die gewährleisten, dass nur berechtigte Personen die Computer der Praxis nutzen können. Z.B.: Passwortschutz, vorherige Autorisierung von Fernwartungen.)

* ..................................
* ..................................

**5. Übermittlung von Patientendaten**

(Maßnahmen, die gewährleisten, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden. Z.B.: Die Praxis sorgt für eine sichere E-Mail-Verbindung. Patientendaten werden nur dann unverschlüsselt über das Internet – via E-Mail oder FAX – verschickt, wenn sich die Patienten damit einverstanden erklärt haben.)

* ..................................
* ..................................

**6. Speicherung und Löschung von Daten**

(Maßnahmen, die gewährleisten, dass die Aufbewahrungsfristen eingehalten und dass die Patientendaten nach Ablauf der Aufbewahrungsfristen zuverlässig gelöscht werden.)

* ..................................
* ..................................

**7. Abläufe in Notfällen**

(Maßnahmen, die einen geregelten Ablauf bei einer Datenpanne gewährleisten. Z.B.: Wer ist für die Meldung an die Datenschutzbehörde zuständig, wenn eine Datenpanne passiert?)

* ..................................
* ..................................

**8. Auftragskontrolle**

(Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Z.B.: Es liegen Datenauftragsverarbeitungsverträge mit den entsprechenden Dienstleistern vor.)

* ..................................
* ..................................

**9. Datenschutz auf Mitarbeiterebene**

(Maßnahmen, die gewährleisten, dass der Datenschutz auch gegenüber den Mitarbeitern gewahrt wird, z.B. Zugriffsbeschränkungen auf Personal- und Abrechnungsdaten, abschließbare Mitarbeiter-Spinde.)

* ..................................
* ..................................

**10. Datenträgerkontrolle**

(Maßnahmen, die verhindern, dass Unbefugten Datenträger lesen, kopieren, verändern oder löschen.)

* ..................................
* ..................................

**11. Speicherkontrolle**

(Maßnahmen, die die unbefugte Eingabe von personenbezogenen Daten sowie die unbefugte Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten gewährleisten.)

* ..................................
* ..................................

**12. Benutzerkontrolle**

(Maßnahmen, die verhindern, dass automatisierte Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte genutzt werden.)

* ..................................
* ..................................

**13. Zugriffskontrolle für sonstige Gerätschaften**

(Maßnahmen, die gewährleisten, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben.)

* ..................................
* ..................................

**14. Übertragungskontrolle**

(Maßnahmen, die gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.)

* ..................................
* ..................................

**15. Eingabekontrolle**

(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.)

* ..................................
* ..................................

**16. Transportkontrolle**

(Maßnahmen, die gewährleisten, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden.)

* ..................................
* ..................................

**17. Wiederherstellbarkeit**

(Maßnahmen, die gewährleisten, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.)

* ..................................
* ..................................

**18. Zuverlässigkeit**

(Maßnahmen, die gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.)

* ..................................
* ..................................

**19. Datenintegrität**

(Maßnahmen, die gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.)

* ..................................
* ..................................

**20. Verfügbarkeitskontrolle**

(Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind.)

* ..................................
* ..................................

**21. Trennbarkeit**

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

* ..................................
* ..................................

**22. Sonstige sicherheitsrelevante Aspekte**

* ..................................
* ..................................