# Praxisinterne Datenschutzrichtlinie – Verzeichnis der allgemeinen technisch-organisatorischen Maßnahmen

Angaben zum Verantwortlichen: [von der Praxis auszufüllen]

Name der Praxis, Straße, Hausnummer, Postleitzahl und Ort einfügen

Telefon, E-Mail-Adresse, Praxisinhaber einfügen

Angaben zum Datenschutzbeauftragten (soweit bestellt)

Name des/der Datenschutzbeauftragten, Telefon, E-Mail-Adresse,

bei externem DSB zusätzlich Straße, Hausnummer, Postleitzahl und Ort

### 1. Rechtliche Rahmenbedingungen

Die Praxis [xxx] ist eine nicht-öffentliche Stelle. Für diese gelten insbesondere die Anforderungen der DS-GVO. Darüber hinaus gibt es bereichsspezifische Spezialgesetze, die gegenüber den Regelungen der DS-GVO vorrangig sind (z.B. Sozialgesetzbuch).

### 2. Zulässigkeit der Verarbeitung von personenbezogenen Daten in der Praxis

Die Verarbeitung personenbezogener (bzw. -beziehbarer) Daten ist nur zulässig, wenn eine Rechtsvorschrift der DS-GVO dies erlaubt. Dieses kann auch die Einwilligung des Betroffenen, also des Patienten oder des Mitarbeiters in der Praxis, sein.

Die Datenverarbeitung in der Praxis hat in der Regel ihre Rechtsgrundlage in Art. 9 DS-GVO i.V.m. § 22 Abs. 1 Nr. 1 Buchst. b BDSG. Weitere Rechtsgrundlagen in der vertragsärztlichen Praxis finden sich in dem Sozialgesetzbuch V. Rechtsgrundlage für die Verarbeitung von Mitarbeiterdaten im Rahmen des Beschäftigtenverhältnisses ist in der Regel § 26 BDSG.

Die Grundsätze der Erforderlichkeit und Zweckbindung der Verarbeitung werden berücksichtigt, indem die personenbezogenen Daten ausschließlich zum Zweck der Aufgabenerfüllung, also der Durchführung der erforderlichen Behandlungsmaßnahmen genutzt werden.

Die Gestaltung und Auswahl der Datenverarbeitungsprogramme in der Praxis richten sich an dem Ziel aus, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Grundsätzlich wird von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch gemacht.

Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden, werden nur für diese Zwecke verwendet. Die Verarbeitung erfolgt nur für die vorher festgelegten Zwecke.

### 3. Datengeheimnis, Verpflichtung auf den Datenschutz, Schulungen

Den mit der Verarbeitung personenbezogener Daten beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Alle Beschäftigten werden bei Aufnahme ihrer Tätigkeit auf das Datengeheimnis und das Berufsgeheimnis verpflichtet. Die Verpflichtung auf das Datengeheimnis und das Berufsgeheimnis schützen besonders die Persönlichkeitsrechte der Betroffenen. Gleichzeitig informieren diese die Mitarbeitenden über ihre Verpflichtung, die Informationen und Daten – insbesondere diejenigen, aus denen sich ein Personenbezug ergibt – in verantwortlicher und berechtigter Weise zu schützen, zu benutzen und weiterzugeben. Die in der Praxis beschäftigten Personen werden durch den Verantwortlichen regelmäßig im Hinblick auf den Datenschutz geschult.

### 4. Technische und organisatorische Maßnahmen in der Praxis zum Schutze der Daten

Zum Schutz der personenbezogenen Daten werden seitens der Praxis die notwendigen technischen und organisatorischen Maßnahmen getroffen, die erforderlich sind, um die Ausführung der Vorschriften der DS-GVO zu gewährleisten. Dabei trifft die Praxis als Verantwortlicher die gemäß Art. 32 DS-GVO erforderlichen technisch-organisatorischen Maßnahmen wie folgt:

### 4.1. Pseudonymisierung

Beschreibung der Maßnahmen, die insbesondere zur Trennung von Patientendaten getroffen wurden.

### 4.2. Verschlüsselung

Beschreibung der Maßnahmen, in welchen Bereichen welche Verschlüsselung gewählt wird.

### 4.3. Vertraulichkeit

Beschreibung der Maßnahmen, insbesondere aus den Bereichen der Zugangs- und Zugriffskontrolle, wie ein unautorisierter Zugang oder Zugriff auf personenbezogene Daten verhindert wird.

### 4.4. Integrität

Beschreibung der Maßnahmen, wie die Integrität der Daten gewährleistet, also eine unbemerkte Änderung von personenbezogenen Daten verhindert wird, Beschreibung des Berechtigungs- und Zugriffskonzepts, der Eingabekontrolle und einer Protokollierung.

### 4.5. Verfügbarkeit

Beschreibung der Maßnahmen, die sicherstellen, dass die personenbezogenen Daten dauernd und uneingeschränkt vorhanden sind, Verfügbarkeitskontrolle, Auftragskontrolle.

### 4.6. Belastbarkeit

Beschreibung der Maßnahmen, die sicherstellen, dass die Systeme derart ausgelegt sind, dass sie jederzeit leistungsfähig bleiben, Speicher-, Zugriffs-, Leitungskapazitäten.

### 4.7. Physischer oder technischer Zwischenfall

Beschreibung der Maßnahmen, die eine rasche Wiederherstellungsmöglichkeit von Systemen und Datenbanken bei physischen oder technischen Zwischenfällen sicherstellen, Backup-Konzepte, Nutzung von Cloud-Services.

### 4.8. Weitere zu ergreifende technische und organisatorische Maßnahmen und deren konkrete Umsetzung werden in gesonderten Dienstanweisungen festgelegt

• Dienstanweisung zur Erteilung von Auskünften an Patienten, Krankenkassen und Dritte

• Dienstanweisung zu Nutzung von PC, Telefon, E-Mail und Internet

• Dienstanweisung zur Vergabe von Passwörtern

### 5. Datenschutzfolgeabschätzung

Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung, voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt die Praxis als Verantwortlicher vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch und dokumentiert deren Ergebnis, Art. 35 DS-GVO.

### 6. Rechte der Betroffenen

Die folgenden Rechte, die die Betroffenen nach der DS-GVO haben, werden durch die Praxis eingehalten:

• Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung

• Widerspruch sowie Datenübertragbarkeit, Art. 15–22 DS-GVO

• Recht zum Widerruf, Art. 7 DS-GVO

• Daneben hat der Betroffene auch das Recht, sich bei der zuständigen Aufsichtsbehörde zu beschweren, Art. 77 DS-GVO

### 7. Verzeichnis der Verarbeitungstätigkeiten

Die DS-GVO verlangt gemäß Art. 30, dass der Verantwortliche ein Verzeichnis aller Verarbeitungstätigkeiten führen muss, das die eingesetzten Verfahren erfasst, mit denen personenbezogene Daten verarbeitet werden. Dieser Anforderung ist die Praxis mit ihrem Verzeichnis aller Verarbeitungstätigkeiten nachgekommen. Dieses Verzeichnis wird intern in regelmäßigen Abständen überprüft.

Stand [von der Praxis auszufüllen]