*[Dieses Dokument stellt beispielhaft dar, wie die technisch-organisatorischen Maßnahmen in einer Apotheke aussehen und dokumentiert werden können. Bitte passen Sie diese auf die Gegebenheiten in Ihrer Apotheke an und holen sich gegebenenfalls Unterstützung bei Ihrem Systemadministrator.]*

**Technische und organisatorische Maßnahmen**

1. **Pseudonymisierung**

Daten werden in einer Weise verarbeitet, dass sie ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Die Pseudonymisierung dient der Datenminimierung.

**Maßnahmen u.a.:**

* Weiterleitung der T-Rezepte entsprechend § 3a AMVV in Verbindung mit der Bekanntmachung des BfArM zur AMVV vom 06.01.2016 ohne Angaben zum Patienten (durch die Vorlage schon vorgegeben)
1. **Verschlüsselung**

Vorgang, bei dem klar lesbare Informationen mit Hilfe eines Verschlüsselungsverfahrens in eine nicht einfach interpretierbare Zeichenfolge (Geheimtext) umgewandelt werden. Die Verschlüsselung dient der Zweckbindung, der Vertraulichkeit und der Integrität der Daten.

**Maßnahmen u.a.:**

* Einsatz von VPN-Technologie
* verschlüsselter Versand von E-Mails
1. **Gewährleistung der Vertraulichkeit**

Schutz der Systeme und Dienste vor einem unberechtigten Zugriff.

* **Zutrittskontrolle**

Maßnahmen zur Verhinderung unbefugten Zutritts zu Datenverarbeitungsanlagen.

**Maßnahmen u.a.:**

* Schlüsselregelung
* Sicherheitsschlösser
* Alarmanlage
* Lichtschranke / Bewegungsmelder
* Absicherung von Gebäudeschächten
* Sorgfältige Auswahl von Reinigungspersonal
* Sorgfältige Auswahl von Botendienstpersonal
* **Zugangskontrolle**

Maßnahmen zur Verhinderung unbefugten Zugangs zu Datenverarbeitungssystemen.

**Maßnahmen u.a.:**

* sichere Kennwörter
* Authentifikation mit biometrischen Verfahren
* automatische Sperrmechanismen
* Zwei-Faktor-Authentifizierung
* Verschlüsselung von Datenträgern
* Zuordnung von Benutzerrechten
* Erstellen von Benutzerprofilen
* Sperren von externen Schnittstellen (USB etc.)
* Einsatz von Anti-Viren-Software
* Einsatz einer Hardware-Firewall
* Einsatz einer Software-Firewall
* Verschlüsselung von mobilen Datenträgern
* Verschlüsselung von Datenträgern in Laptops/Notebooks
* **Zugriffskontrolle**

Maßnahmen (bei der Verarbeitung, Nutzung und nach der Speicherung) zur Verhinderung unbefugter Kenntniserlangung sowie unbefugten Lesens, Kopierens, Veränderns oder Entfernens innerhalb des Systems.

**Maßnahmen u.a.:**

* Diskretionsabstand
* Nichteinsehbarkeit der PC-Bildschirme durch Nichtapothekenpersonal
* Arbeitsanweisung zum Umgang mit dem Faxeingang/Faxsendeberichten
* Arbeitsanweisung zum Umgang mit Verordnungen und liegengelassenen Rechnungen
* Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte
* 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
* ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
* Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
* Protokollierung der Vernichtung
* **Trennungskontrolle**

Daten, die zu unterschiedlichen Zwecken erhoben wurden, werden getrennt verarbeitet.

**Maßnahmen u.a.:**

* physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
* Logische Kundentrennung (softwareseitig)
* Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
* Versehen der Datensätze mit Zweckattributen/Datenfeldern
* Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
* Erstellung eines Berechtigungskonzepts und Festlegung von Datenbankrechten
1. **Gewährleistung der Integrität**

Schutz der Systeme und Dienste vor (unerkannter) Manipulation.

* **Weitergabekontrolle**

Maßnahmen, die ein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport verhindern.

**Maßnahmen u.a.:**

* Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
* Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
* Einrichtungen von Standleitungen bzw. VPN-Tunneln
* Weitergabe von Daten in anonymisierter/pseudonymisierter Form
* E-Mail-Verschlüsselung/E-Mail-Filter
* Softwareupdates
* Antivierensoftware
* bei physischem Transport: sichere Transportbehälter/- verpackungen
* bei physischem Transport: sorgfältige Auswahl von Transportpersonal und -fahrzeugen
* elektronische Signatur
* **Eingabekontrolle**

Maßnahmen zur Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

**Maßnahmen u.a.:**

* Protokollierung der Eingabe, Änderung und Löschung von Daten
* Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
* Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
* Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
* Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
1. **Gewährleistung der Verfügbarkeit**

Sicherstellung, dass die Daten über das System/den Dienst jederzeit genutzt/abgerufen werden können. Maßnahmen zum Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust (Verfügbarkeitskontrolle).

**Maßnahmen u.a.:**

* Backup-Strategie (online/offline; on-site/off-site)
* Testen von Datenwiederherstellung
* Unterbrechungsfreie Stromversorgung (USV)
* Klimaanlage in Serverräumen
* Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
* Schutzsteckdosenleisten in Serverräumen
* Feuer- und Rauchmeldeanlagen
* Feuerlöschgeräte in Serverräumen
* Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
* Serverräume nicht unter sanitären Anlagen
* In Hochwassergebieten: Serverräume über der Wassergrenze
* Virenschutz
* Firewall
* Meldewege und Notfallpläne
* Maßnahmen zur raschen Wiederherstellbarkeit der Daten
1. **Gewährleistung der Belastbarkeit der Systeme und Dienste**

Die Fähigkeit von Systemen und Diensten, mit Veränderungen umzugehen.

**Maßnahmen u.a.:**

* RAID-System (redundante Anordnung unabhängiger Festplatten)
1. **Verfügbarkeit der und Zugang zu den Daten**

Die Verfügbarkeit und der Zugang zu den Daten bei einem (nicht alltäglichen) physischen oder technischen Zwischenfall sollen schnell wiederherzustellen sein.

**Maßnahmen u.a.:**

* Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort (z.B. Rechenzentren)
* Backup- und Recovery-Strategien
1. **Kontrollverfahren**

Mittelbare Herstellung von Datensicherheit durch regelmäßige Kontrolle der unmittelbar wirkenden Maßnahmen.

* **Interne Kontrolle**

Maßnahmen, die gewährleisten, dass die unmittelbar wirkenden Maßnahmen zum Schutz der intern verarbeiteten personenbezogenen Daten ihre Funktion erfüllen.

**Maßnahmen u.a.:**

* Maßnahmenkonzept zur Überprüfung, Bewertung und Evaluierung der Wirksamkeit der etablierten Maßnahmen
* **Auftragskontrolle**

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

**Maßnahmen u.a.:**

* Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
* vorherige Prüfung und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
* schriftliche Weisungen an den Auftragnehmer (durch einen Vertrag zur Auftragsverarbeitung) im Sinne des Art. 28 DSGVO
* Verpflichtung des Auftragsverarbeiters, seine Mitarbeiter auf das Datengeheimnis zu verpflichten
* ein durch den Auftragsverarbeiter benannter Datenschutzbeauftragter
* Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
* Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragsverarbeiter
* laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
* Vertragsstrafen bei Verstößen
1. **Anweisung durch den Verantwortlichen**

Personelle Maßnahmen, die u.a. sicherstellen, dass die Datenverarbeitung nur auf Anweisung des Verantwortlichen erfolgt.

**Maßnahmen u.a.:**

* Betriebs- und Dienstanweisungen
* Weisungen bezogen auf den Einzelfall
* Verpflichtung der Mitarbeiter auf den Datenschutz
* Auswahl der Person, welche die Datenverarbeitung vornehmen soll, nach dem Kriterium ihrer (potentiellen) Zuverlässigkeit

**Schriftliche Dokumentation von Maßnahmen:**

* Datenschutzanweisung gegenüber Mitarbeitern/Betriebs- und Dienstanweisungen
* IT-Sicherheitszertifizierung
* Verpflichtungen auf den Datenschutz
* u.a.

………………………………………..

Ort, Datum

………………………………………..

Unterschrift des Verantwortlichen