

# IT-SICHERHEITSPRÜFLISTE FÜR APOTHEKEN - MUSTERANFORDERUNGEN

Version	Datum	Kurzbeschreibung	Durchgeführt von
1.0	01.08.2025	Erstversion	ABDA

**Hinweis:**

Bei konkreten Fragen zu Ihrer Apotheke kontaktieren Sie ihren IT-Dienstleister. Bei Fragen zur Verwendung oder Weitergabe des Dokuments wenden Sie sich bitte an die ABDA – Bundesvereinigung Deutscher Apothekerverbände e.V.

## **Inhaltsverzeichnis**

Inhaltsverzeichnis .....	3
Musteranforderungen an eine Apotheke.....	4
Ausfüllanleitung .....	4
Umgang mit nicht erfüllten Anforderungen.....	4
1. Zutrittskontrolle .....	5
2. Zugangskontrolle .....	6
3. Zugriffskontrolle – Maßnahmen zur Verhinderung von unbefugten Zugriffen .....	8
4. Weitergabekontrolle – Maßnahmen zur Datenübertragung und -weitergabe.....	9
5. Eingabekontrolle – Maßnahmen für Datenkorrektheit und -herkunft.....	10
6. Auftragskontrolle - Maßnahmen zur Qualitätssicherung von Auftragsverarbeitung (AV) .....	11
7. Verfügbarkeitskontrolle und Wiederherstellbarkeit – Maßnahmen zur Geschäftsfortführung nach Sicherheitsvorfall .....	13
8. Datenträgerkontrolle – Maßnahmen zur Verhinderung von Datenverlust auf physischer Ebene .....	16
9. System- und Datenintegrität .....	18

## Musteranforderungen an eine Apotheke

Dieses Dokument dient der Erfassung Ihrer aktuell umgesetzten technischen und organisatorischen Maßnahmen (TOMs) in Bezug auf Datenschutz und IT-Sicherheit. Es soll lediglich als Orientierung und Hilfestellung für Apotheken dienen, die ihre Datenverarbeitungssysteme im Hinblick auf Datenschutz und IT-Sicherheit optimieren möchten.

Für nicht erfüllte Maßnahmen sollten Sie, gegebenenfalls mit Ihrem jeweiligen IT-Dienstleister, planen, wie Sie angemessene Schutzmaßnahmen in Ihrer Apotheke einführen können.

## Ausfüllanleitung

Im Folgenden finden Sie eine Übersicht über die technischen und organisatorischen Maßnahmen. Sollten bestimmte Maßnahmen für Ihre Apotheke nicht anwendbar sein, können diese als „nicht anwendbar“ (N/A) mit einer entsprechenden Erklärung gekennzeichnet werden.

Zur Bewertung der Umsetzung gibt es drei Erfüllungsgrade:

1. **Ja** (Maßnahme ist erfüllt)
2. **Nein** (Maßnahme ist nicht oder nur teilweise erfüllt)
3. **N/A** (Maßnahme ist für Ihre Apotheke nicht relevant; etwa, weil Sie keine entsprechenden Systeme betreiben)

Falls für einzelne Maßnahmen weitere Angaben zu den Erfüllungsgraden erforderlich sind, finden Sie diese jeweils am Ende der entsprechenden Zeile.

Wenn Sie mehrere IT-Systeme betreiben, sollte eine Maßnahme für jedes System geprüft werden. Systeme, bei denen die Maßnahme nicht eingeführt ist, vermerken Sie in der Spalte „Erklärung“; und wählen als Antwort „Nein“ aus.

## Umgang mit nicht erfüllten Anforderungen

In der Praxis wird kaum eine Apotheke alle aufgeführten Maßnahmen vollständig umsetzen. Das ist auch nicht Ziel dieser Checkliste. Vielmehr sollen damit Risiken und mögliche Lücken in der IT-Sicherheit Ihrer Apotheke identifiziert werden. Wenn Sie bei einzelnen Maßnahmen „Nein“ oder „N/A“ angegeben haben, bewerten Sie anschließend, ob die Nichterfüllung einer Maßnahme ein akzeptables Risiko für Ihre Apotheke darstellt oder ob hier Handlungsbedarf besteht. Ziehen Sie im Zweifel Ihre zuständigen IT-Dienstleister hinzu, um gemeinsam eine sinnvolle Priorisierung der Maßnahmen festzulegen. Es empfiehlt sich, Verantwortlichkeiten für die Umsetzung bereits im Vorfeld klar zu definieren. Als Hilfestellung hierzu finden Sie eine Übersicht in Kapitel 4 (Tabelle 1) des Dokuments „Hinweise für ein IT-Sicherheitskonzept für Apotheken“.

## 1. Zutrittskontrolle

Mit der Zutrittskontrolle sind alle Maßnahmen gemeint, die unbefugten Personen den Zutritt auf Geländen, Gebäuden oder Räumlichkeiten verbieten oder durch Überwachung zur Erkennung beitragen können.

Nr.	Maßnahmen	Hinweise, Realisierungsmöglichkeiten	Wie umgesetzt, wo dokumentiert, weitere Anmerkungen	Ja	Nein	N/A
1.1	Zutrittsberechtigungskonzept	Dokument, das beschreibt, welche Personen oder Rollen wo zu welchem Zweck Zutritt haben		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.2	Zutrittskontrollsystem	Möglichkeiten u.a.: <ul style="list-style-type: none"> <li>- Personengestützt (Portier, ...)</li> <li>- Mechanisch (Schlösser)</li> <li>- Mechatronisch (Schlösser + Elektronik)</li> <li>- Digital (Zutrittskarten, biometrisch wie Fingerabdruck)</li> </ul>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.3	Zutrittsüberwachung	Möglichkeiten u.a. (auch mehrere): <ul style="list-style-type: none"> <li>- Nur durch Zutrittskontrollsystem</li> <li>- Alarmanlage (mit /ohne Sicherheitsdienst)</li> </ul> Kameraüberwachung (mit / ohne Aufzeichnung)		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## 2. Zugangskontrolle

Bei der Zugangskontrolle geht es um die Verhinderung der unbefugten Nutzung von bspw. Computern sowie deren Überwachung. Diese sollen nur von Personen mit einer entsprechenden Befugnis zur Nutzung verwendet werden.

Nr.	Maßnahmen	Hinweise, Realisierungsmöglichkeiten	Wie umgesetzt, wo dokumentiert, weitere Anmerkungen	Ja	Nein	N/A
2.1	Dokumentation für Zugang zu IT-Systemen	<ul style="list-style-type: none"> <li>- Mögliche Maßnahmen: Passwortrichtlinien mit Überprüfung</li> <li>- Dokumentation von technischen Absicherungsmaßnahmen (bspw. Konfiguration von Firewalls, TI-Konnektor(en), etc.)</li> </ul>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.2	Aufstellung von Regeln für Firmenfremde	<p>Möglichkeiten u.a. (auch mehrere):</p> <ul style="list-style-type: none"> <li>- Erstunterweisung für Verhalten in Hinblick auf Datenschutz</li> <li>- kein unbeaufsichtigter Zugang zu sensiblen Bereichen</li> </ul>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.3	Authentisierung für IT-Systeme	<p>Möglichkeiten u.a. (auch mehrere):</p> <ul style="list-style-type: none"> <li>- Benutzername + Passwort</li> <li>- Passkeys</li> </ul>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

2.4	Protokollierung des Fernzugangs per VPN u. Ä.	<p>Wichtige Informationen u.a.:</p> <ul style="list-style-type: none"> <li>- Aufbewahrungsdauer der Protokolle (möglichst mehr als 30 Tage) für den Schadensfall</li> </ul>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.5	Bildschirmsperre für alle Rechner	<p>Wichtige Informationen u.a.:</p> <ul style="list-style-type: none"> <li>- Automatische Sperrung nach möglichst max. 15 min</li> <li>- Mitarbeiteranweisung zur Sperrung bei Verlassen des Rechners</li> </ul>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### 3. Zugriffskontrolle – Maßnahmen zur Verhinderung von unbefugten Zugriffen

Durch die Zugriffskontrolle wird gewährleistet, dass niemand über seine Berechtigung hinaus Daten verarbeiten kann.

Nr.	Maßnahmen	Hinweise, Realisierungsmöglichkeiten	Wie umgesetzt, wo dokumentiert, weitere Anmerkungen	Ja	Nein	N/A
3.1	IT-Systeme mit Rollenkonzept	Möglichkeiten u.a. (ggf. verschieden je IT-Anwendung): <ul style="list-style-type: none"> <li>- Benutzer in Software verwaltet, Rechte zugewiesen</li> <li>- Benutzer auf Betriebssystem- oder Rechnergruppen- (Domänen)-Ebene verwaltet, Rechte in Applikation zugewiesen</li> <li>- Benutzer auf Betriebssystem- oder Rechnergruppen- (Domänen)-Ebene verwaltet, Rechte über zentralen Verzeichnisdienst zugewiesen</li> <li>- Standard-Werte für Zugänge (Benutzername und / oder Passwort) wurden abgeändert.</li> </ul>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.2	Berechtigungen auf Funktionsebene feingranular steuerbar	z.B. Fakturierung oder Mitarbeiterverwaltung nur von privilegierten Benutzern aufrufbar		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## 4. Weitergabekontrolle – Maßnahmen zur Datenübertragung und -weitergabe

Mit der Weitergabekontrolle sind Maßnahmen gemeint, die die Sicherheit von Daten während einer Datenweitergabe gewährleisten. Unter Datenweitergabe in diesem Sinne sind elektronische Übertragungen oder physischer Transport auf Datenträgern zu verstehen.

Nr.	Maßnahmen	Hinweise, Realisierungsmöglichkeiten	Wie umgesetzt, wo dokumentiert, weitere Anmerkungen	Ja	Nein	N/A
4.1	Technische Protokollierung von Datenübertragungen	Nötig für die Übertragung kritischer Daten (personenbezogene sowie vertrauliche Daten) insbesondere Warenwirtschaft, Laborsysteme		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.2	Firewall-Richtlinie	- Bereitstellung und Dokumentation durch IT-Dienstleister/AVS		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.3	Zugangsbeschränkung für Fernzugriffe	- Nur in Abstimmung mit dem IT-Dienstleister / AVS		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.4	Sicherung kritischer physischer Übertragungswege	Maßnahmen z.B.: - Postbuch - Briefsiegel - Gesicherte Transportbehälter		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## 5. Eingabekontrolle – Maßnahmen für Datenkorrektheit und -herkunft

Bei der Eingabekontrolle geht es um die Überprüfbarkeit der Datenverarbeitung. Durch entsprechende Maßnahmen soll die Kontrolle von Dateneingaben, Datenveränderungen und Datenlöschungen gewährleistet werden. Durch das Integrieren dieser Maßnahme kann genau überprüft werden, wer welche Daten innerhalb der Systeme eingegeben, verändert oder gelöscht hat.

Nr.	Maßnahmen	Hinweise, Realisierungsmöglichkeiten	Wie umgesetzt, wo dokumentiert, weitere Anmerkungen	Ja	Nein	N/A
5.1	Löschkonzept	Maßnahmen u.a.: <ul style="list-style-type: none"> <li>- Realisierung notwendiger Funktionen gemäß DSGVO (Löschen, Sperren)</li> <li>- Überschreiben von Backup-Datenträgern</li> </ul> Siehe auch Datenträgervernichtung unter „8. Datenträgerkontrolle – Maßnahmen zur Verhinderung von Datenverlust auf “.		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## 6. Auftragskontrolle - Maßnahmen zur Qualitätssicherung von Auftragsverarbeitung (AV)

Immer dann, wenn eine Auftragsverarbeitung (ob für personenbezogene Daten lt. DSGVO oder für andere Daten) stattfindet, muss gewährleistet werden, dass die Verarbeitung nach den Weisungen des Auftraggebers erfolgt.

Nr.	Maßnahmen	Hinweise, Realisierungsmöglichkeiten	Wie umgesetzt, wo dokumentiert, weitere Anmerkungen	Ja	Nein	N/A
6.1	Schriftliche Weisungen für nachzuweisende Aufträge	Maßnahmen u.a.: <ul style="list-style-type: none"> <li>- Verwendung elektronischer Kommunikation für wichtige Aufträge (z.B. Ticketsysteme)</li> <li>- Verwendung unveränderbarer Kommunikation für kritische Aufträge (z.B. signierte E-Mails)</li> </ul>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.2	Auftragsverarbeitungsvertrag (AVV)	Überprüfung, ob ein AVV vorliegt und Regeln zum Umgang mit den Daten in jedem denkbaren Fall und Beschreibung der beim Auftragnehmer umgesetzten TOMs enthält. Siehe auch Art. 28 DSGVO.		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.3	Regelmäßige TOM-Kontrolle	Bei längerer Zusammenarbeit: Laufende Überprüfung des		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

		Auftragnehmers und seines Schutzniveaus				
<b>6.4</b>	Vorhandene oder vorgeschriebene Zertifizierungen kontrollieren	Nachweise durch den Auftragnehmer		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>6.5</b>	Verantwortlichkeiten bei Auftragsverarbeitungen festlegen	Maßnahmen u.a.: <ul style="list-style-type: none"> <li>- Auftragskommunikation festlegen (z.B. Ticketsystem, Telefonsupport)</li> <li>- Ansprechpartner und Vertreter bestimmen</li> </ul>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## 7. Verfügbarkeitskontrolle und Wiederherstellbarkeit – Maßnahmen zur Geschäftsfortführung nach Sicherheitsvorfall

Bei der Verfügbarkeitskontrolle und Wiederherstellbarkeit müssen Daten gegen Zerstörung oder Verlust geschützt werden, damit diese im Störfall wiederhergestellt werden können.

Nr.	Maßnahmen	Hinweise, Realisierungsmöglichkeiten	Wie umgesetzt, wo dokumentiert, weitere Anmerkungen	Ja	Nein	N/A
7.1	Kontrolle der Datenträger und Datensicherungen	Maßnahmen u.a.: <ul style="list-style-type: none"> <li>- Regelmäßige manuelle Wiederherstellungstests</li> <li>- Systemfunktionen zur Überprüfung von Datenträgern und -sicherungen regelmäßig ausführen</li> </ul>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.2	Kontrolle bzw. Monitoring der technischen Einrichtungen	Maßnahmen u.a.: <ul style="list-style-type: none"> <li>- Vorhandensein und regelmäßige Prüfung von z.B. Notstromaggregaten, Überspannungsschutzeinrichtungen, Geräte für unterbrechungsfreie Stromversorgung (USV), Brandmelder/Feuerlöscher</li> </ul>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.3	Kontrolle Notfallkonzepte	Vorhandensein eines Notfallkonzeptes zur		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

		Wiederherstellung einer Betriebsfähigkeit, siehe bspw. Checkliste Stromausfall des Deutschen Apothekerverbandes e.V.			
<b>7.4</b>	Notfallübungen	Durchführung von Notfallübungen		<input type="checkbox"/>	<input type="checkbox"/>
<b>7.5</b>	Datensicherungs-konzept	Inhalt u.a. <ul style="list-style-type: none"> <li>- Prozesse zur Sicherung lokaler und entfernter Daten beschreiben</li> <li>- Beschreibung der Schutzmaßnahmen für Datensicherungen</li> <li>- Beschreibung der Wiederherstellungsprozesse</li> <li>-</li> </ul>		<input type="checkbox"/>	<input type="checkbox"/>
<b>7.6</b>	Support-Verfügbarkeit	Maßnahmen u.a. <ul style="list-style-type: none"> <li>- Vereinbarung mit Dienstleistern über Support-Verfügbarkeit (Erreichbarkeit, Antwortzeit)</li> <li>- Rufbereitschaft für kritische Vorfälle / zeitkritische Themen (v.a. Notfälle)</li> </ul>		<input type="checkbox"/>	<input type="checkbox"/>
<b>7.7</b>	Verfügbarkeit von Support / Reparatur-Service-Techniker	Maßnahmen u.a. <ul style="list-style-type: none"> <li>- Vereinbarung mit Dienstleistern über</li> </ul>		<input type="checkbox"/>	<input type="checkbox"/>

		<p>Techniker-Verfügbarkeit (Erreichbarkeit, Antwortzeit)</p> <ul style="list-style-type: none"> <li>- Geplante Ersatzteilhaltung für wichtige IT- und andere Einrichtungen</li> </ul>				
<b>7.8</b>	Schadsoftware-Erkennung und -bewältigung	<p>Maßnahmen u.a.</p> <ul style="list-style-type: none"> <li>- Anti-Viren-Schutz</li> <li>- Anti-Spam-Schutz</li> <li>- Anti-Phishing-Schutz</li> <li>- Monitoring-Systeme für Datenflüsse</li> <li>- Monitoring-Systeme für extern erreichbare Schnittstellen, Login-Versuche und Abgriff von Passworten</li> </ul>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>7.9</b>	Feuer – und Rauchmeldeanlagen, Brandlöschung	Schnelle Erkennung und Reaktion auf Brände		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## 8. Datenträgerkontrolle – Maßnahmen zur Verhinderung von Datenverlust auf physischer Ebene

Bei der Datenträgerkontrolle geht es um die Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern.

Nr.	Maßnahmen	Hinweise, Realisierungsmöglichkeiten	Wie umgesetzt, wo dokumentiert, weitere Anmerkungen	Ja	Nein	N/A
8.1	Verschlüsselung für mobile Datenträger	Maßnahmen u.a.: - Verschlüsselung von USB-Sticks (z.B. Bitlocker)		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.2	Verschlüsselung für Geräte	Bspw. Festplattenverschlüsselung für mobile Geräte (z.B. Bitlocker)		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.3	Sichere Aufbewahrung	Siehe Abschnitt „Gesicherte Lagerung von Datensicherungen“ unter 7. Verfügbarkeitskontrolle		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.4	Löschschutz	Maßnahmen u.a. - Verzeichnisse und Dateien mit Betriebssystem-Standard-Löschschutz versehen		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

		<ul style="list-style-type: none"> <li>- Applikationslogik für Löschschutz einsetzen (Löschrecht entziehen)</li> <li>- Anlegen von Schattenkopien oder Datensicherungen für das Zurückspielen bei versehentlichem Löschen</li> </ul>				
8.5	Physische Löschung von Datenträgern	<p>Maßnahmen u.a.</p> <ul style="list-style-type: none"> <li>- sicheres Löschen von Datenträgern mit zertifizierten Löschttools mit Ergebnisprotokollierung</li> <li>- Schreddern von Datenträgern durch zertifizierte Datenträgervernichtungsunternehmen</li> </ul>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## 9. System- und Datenintegrität

Die System- und Datenintegrität beinhaltet die Sicherstellung, dass gespeicherte Daten nicht durch Fehlfunktionen des Systems beschädigt oder manipuliert werden können.

Nr.	Maßnahmen	Hinweise, Realisierungsmöglichkeiten	Wie umgesetzt, wo dokumentiert, weitere Anmerkungen	Ja	Nein	N/A
9.1	Updates Betriebssystem und Firmware	Maßnahmen u.a. <ul style="list-style-type: none"> <li>- Aktivierung automatisierter Updates</li> <li>- Update-Durchführung durch Auftragsverarbeiter</li> </ul>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.2	Updates Software	Maßnahmen u.a. <ul style="list-style-type: none"> <li>- Aktivierung automatisierter Updates z.B. für Standard-Software</li> <li>- Update-Durchführung durch Systemanbieter</li> </ul>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>