Die wichtigsten Datenschutztipps für Apotheker

In diesem Leitfaden finden Sie die wichtigsten Informationen und Prüfschritte für Ihre Apotheke

Es ist recht selbstverständlich, dass in Apotheken tagtäglich sensible personenbezogene Daten erhoben und gespeichert werden. Was hingegen nicht überall so selbstverständlich ist: Die sichere Datenverarbeitung. E-Rezept, Onlineshops, Videoüberwachung in der Offizin, Diskretionsabstände.

Warum sind die in Apotheken verarbeiteten Daten besonders sensibel?

Personenbezogene Daten sind der Dreh- und Angelpunkt der DSGVO. In Artikel 4 werden sie definiert als „alle Informationen, die sich auf eine […] identifizierbare natürliche Person […] beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu […] einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen […] Identität dieser natürlichen Person sind."

Innerhalb dieser personenbezogenen Daten gibt es eine Kategorie „besonders schützenswerter Daten", die Rückschluss auf die Lebensführung zulassen. Unter anderem eben auch genetische Informationen oder Krankendaten – also genau solche Informationen, die Ihnen Ihre Kunden offenlegen, wenn sie

- **ein Rezept einlösen,**
- **Medikamente bestellen oder**
- **um Beratung bitten.**

Damit nun keine Unbefugten Einblick in diese Daten erhalten (und sei es nur, weil Ihr Mitarbeiter einen Medikamentennamen laut durch den Raum ruft), sind Sie als Besitzer der Apotheke zum Datenschutz angehalten. Niemand möchte schließlich, dass intime Gesundheits-Informationen in falsche Hände gelangen. Andernfalls droht Ihnen neben hohen Bußgeldern auch der Vertrauensverlust vonseiten Ihrer Kunden.

Wo finde ich Vorgaben zum Datenschutz in Apotheken?

An erster Stelle natürlich in der europäischen Datenschutz-Grundverordnung (DSGVO), die Datenschutzfragen branchenübergreifend regelt. Für Ihren Internetauftritt finden Sie ergänzende Vorgaben im Telekommunikation-Telemedien-Datenschutzgesetz

- (TTDSG). Speziell für Apotheken gelten darüber hinaus diese Richtlinien:
- Sozialgesetzbuch (SGB)
- Apothekenbetriebsordnung (ApBetrO)
- Patientendaten-Schutz-Gesetz (PDSG)
- Heilberufe-Kammergesetz bzw. Kammergesetz für die Heilberufe/Kammergesetz/Heilberufsgesetz

Grundlagen des Datenschutzes

Datenerhebung

- In meiner Datenschutzerklärung (Aushang in der Offizin sowie auf der Webseite eingebunden) finden Kunden einen Hinweis, an wen die Daten übermittelt werden.
- Sofern ich Tools oder PlugIns aus Drittländern wie den USA nutze, weise ich in meiner Datenschutzerklärung noch einmal explizit darauf hin.
- Meine Kunden erfahren auch, zu welchen Zwecken ich die Daten einsammle und an Dienstleister weiterleite.
- Ich gebe an, wie lange ich Daten speichere bzw. was ausschlaggebend dafür ist, dass sie gelöscht werden.
- Ich kläre meine Kunden über ihre Rechte auf – zum Beispiel das Recht auf Auskunft oder Beschwerde.
- **Ich führe ein Verzeichnis meiner Verarbeitungstätigkeiten und Auftragsverarbeitung, um im Falle einer Datenschutz-Rückfrage meiner Rechenschaftspflicht nachzukommen.**

IT-Sicherheit

- Auf den Computern und mobilen Endgeräten in meinem Unternehmen ist Antiviren- und Security-Software installiert.
- Ich habe eine Firewall eingerichtet.
- Die Kommunikation läuft verschlüsselt.
- Meine Mitarbeiter und ich verwenden sichere Passwörter, die auch geschützt aufbewahrt werden.
- Ich führe regelmäßig anstehende Updates meiner Software durch.
- Digitale Daten sind vor Fremdzugriff und -bearbeitung geschützt.

zu IT-Sicherheit

Meine Mitarbeiter sind mit grundlegender Cybersecurity vertraut und wissen z. B., dass nicht achtlos E-Mail-Anhänge geöffnet und Daten weitergegeben werden dürfen.

Die Übermittlung von Abrechnungsdaten an Krankenkassen erfolgt über sichere Wege, z.B. ein gesondertes Online-Portal, spezielle Software oder eine sonstige Schnittstelle.

Offline-Datenschutz

Kundendaten, Patientenbögen und Rezepte lagern wir geschützt: Abschließbare Aktenschränke und Türen zählen ebenso dazu wie beispielsweise Zugangsbeschränkungen.

Überwache ich meine Apotheke per Video, weise ich Kunden ausdrücklich und klar erkennbar darauf hin.

Umgang mit Kundendaten

- Daten werden nur entsprechend der Richtlinien sicher verarbeitet.
- Wir löschen unsere Kundendaten, sobald wir sie nicht mehr brauchen. Werden sie länger aufbewahrt (zum Beispiel für eine Kundenkartei oder Stammkunden-Karten) sprechen wir das vorher mit dem Kunden ab und holen uns schriftlich sein Einverständnis ein. Das gilt sowohl für digitale als auch für analoge Daten.
- **Die Datenschutzerklärung ist vollständig einsehbar – offline auf Papier (z.B. als Ausdruck an der Verkaufstheke) oder auch als Online-Dokument (klassisch verlinkt oder mit QR-Code).**
- **Es gibt einen Plan, was im Falle einer Datenpanne zu tun ist.**
- Sofern ich auf unserer Webseite tracke, Marketing-Pixel nutze oder Daten in die USA weiterleite, hole ich mir die Einwilligung der Webseiten-Nutzer ein.
- **Kunden und Webseiten-Nutzer können ihre Einwilligung zur Datenerhebung jederzeit widerrufen.**

Mitarbeiter

- Meine Mitarbeiter wurden für den sicheren Umgang mit Daten sensibilisiert. Sie wissen, dass sie sensible Patientendaten nicht achtlos weitergeben oder offen zugänglich liegen lassen sollten. Sie sind sich auch bewusst, dass die Gesundheitsinformationen und Medikamente der Kunden Privatsache ist.
- Meine Mitarbeiter werden regelmäßig geschult.
- Es wird regelmäßig überprüft, ob jeder die Vorgaben einhält.

Relevante Artikel der DSGVO

Artikel 5 und 7 – die sichere Datenverarbeitung

Setzen Sie auf Ihre Webseite ein **Consent Banner** (die allseits bekannte Cookie-Box). Dort müssen Nutzer auswählen, inwiefern sie der **Datenverarbeitung zustimmen** und dies bestätigen. Eine **stillschweigende Vereinbarung** à la „Mit der Nutzung unserer Webseite stimmen Sie der Verwendung von Cookies zu“ ist **nicht zulässig**. Nutzer haben das Recht, der Angabe nicht notwendiger Daten zu **widersprechen**. Wer sich für einen Newsletter anmeldet, ist demnach nicht verpflichtet, unnötige Daten wie Alter oder Telefonnummer anzugeben. Zudem sind Sie dazu angehalten, die **Daten sicher aufzubewahren und sie zu löschen**, sobald sie nicht mehr benötigt werden.

Artikel 6 – Rechtmäßigkeit der Datenverarbeitung

Daten dürfen Sie nicht grundlos erheben. Die Datenverarbeitung ist nur dann rechtmäßig, wenn bestimmte Bedingungen erfüllt sind. Für Sie dürfte es mit Bedingung b) Die Verarbeitung ist für die Erfüllung eines Vertrags oder zur Durchführung vorvertraglicher Maßnahmen erforderlich getan sein.

Artikel 13 und 14 – Informationspflicht bei der Datenerhebung

Teilen Sie Kunden direkt zu Beginn der Datenerhebung (zum Beispiel per Hinweis auf Ihre vollständige Datenerklärung) alle relevanten Informationen zur Datenerhebung mit: Name und Kontaktdaten des Datenschutzverantwortlichen, seines Vertreters und ggf. des Datenschutzbeauftragten, Zwecke und Rechtsgrundlage Ihrer Datenerhebung, Empfänger und Datenübermittlung, Speicherdauer und Betroffenenrechte. Auch über indirekte Erhebung wollen Ihre Kunden informiert werden. Das ist beispielsweise der Fall, wenn Sie die Kundenadresse an ein weiteres Handwerksunternehmen weitergeben, das mit Ihnen an diesem Auftrag arbeitet.

Artikel 12, 15 und 30 – Transparenz der Datenverarbeitung

Legen Sie in Ihrer Datenschutzerklärung fest, wozu und auf welche Weise Sie Daten speichern und verarbeiten. Das gilt auch für sämtliche **soziale Netzwerke**, auf denen Ihr Unternehmen unterwegs ist – denn auch dort sammeln Sie beispielsweise mit dem Facebook Pixel Daten. Legen Sie sich außerdem eine Musterauskunft bereit und **protokollieren Sie die Datenverarbeitung** sorgfältig. So kommen Sie leichter Ihrer Pflicht nach, auf Anfrage **innerhalb von vier Wochen** eine Übersicht aller gespeicherten Daten einer Person herausgeben zu können.

Artikel 25 und 32 – technische Voraussetzungen zur Datensicherheit

Stellen Sie durch Firewalls und geeignete Software sicher, dass **keine unbefugten Personen Zugriff** auf die personenbezogenen Daten haben. Außerdem müssen Sie Sorge tragen, **dass sämtliche von Ihnen genutzte Tools** tatsächlich nur die Daten sammeln und auf eine Weise verarbeiten, wie Sie nach Artikel 12 bzw. 30 angeben. Diese müssen so gespeichert werden, dass sie keinen Rückschluss auf bestimmte Personen zulassen – also **pseudonymisiert und verschlüsselt**. Sie sind angehalten, die Sicherheit Ihrer Maßnahmen regelmäßig zu **überprüfen** und – falls nötig – anzupassen.

Artikel 28 – die Weitergabe von Daten

Mit jedem Dienstleister bzw. Unternehmen, an das Sie personenbezogene Daten weiterreichen, müssen Sie einen sogenannten **Auftragsverarbeitungsvertrag** abschließen. Dort wird festgehalten, dass die Daten DSGVO-konform verarbeitet werden. Bei diesem Artikel gilt: Augen auf! Denn darunter fallen auch **gängige Tools** wie Google Analytics – und **Ihr Webhosting-Anbieter**. Viele Dienstleister wie Zoom erstellen diese Vereinbarung automatisch.

Artikel 33, 34 und 35 – Handeln bei Datenpannen

Innerhalb **von 72 Stunden** müssen Sie die Verletzung des Datenschutzes an **Ihre zuständige. Aufsichtsbehörde melden**. Beschreiben Sie, welche Daten auf welche Weise verletzt wurden, geben Sie dabei Ihren Datenschutzbeauftragten an und schätzen Sie ab, welche Folgen diese Verletzung hat. Schlagen Sie zudem Maßnahmen vor, wie Sie mit den Folgen umgehen und die Verletzung beheben. Da dies sehr aufwendig sein kann, legen Sie sich am besten schon im Vorfeld einen Notfall-Plan zurecht, an dem sich alle Involvierten orientieren können.

Artikel 37 – Ernennen eines Datenschutzbeauftragten

Grundsätzlich gilt die DSGVO für alle Unternehmen und Selbstständige, die mit personenbezogenen Daten umgehen. Besonders, wenn Sie sehr sensible Daten verarbeiten, **lohnt sich ein Datenschutzbeauftragter auch schon unter 20 Beschäftigten**. Sie haben die freie Wahl zwischen einem internen und einem externen Beauftragten. **Da ein interner DSB jedoch auch immer noch andere Aufgaben wahrnehmen muss, liegt sein Fokus nicht allein auf dem Datenschutz** und es können ihm Fehler unterlaufen.

➔ **Deshalb empfehlen wir Ihnen, einen zertifizierten externen Partner zu beauftragen**