Datenschutz-Checkliste für Arztpraxen

Im Jahr 2020 haben die deutschen Datenschutzbehörden Bußgelder in Höhe von 46 Mio. EUR festgesetzt. Arztpraxen gehen mit vielen besonders schutzwürdigen Gesundheitsdaten um. Sie müssen damit rechnen, von Behörden besonders genau überprüft zu werden und riskieren im Falle eines Verstoßes - mehr als andere Akteure - empfindliche Bußgelder.

Ist Ihre Arztpraxis im Datenschutz ausreichend aufgestellt? Unsere **Checkliste für Arztpraxen** hilft Ihnen, den Überblick über die Datenschutz-Aufgaben in einer Arztpraxis zu behalten. Sollten Sie eine der folgenden Aufgaben noch nicht erfüllt haben, empfehlen wir, dies zeitnah nachzuholen.

Datenschutz-Aufgaben für Arztpraxen

- ☐ Verarbeitungsverzeichnis erstellen und aktuell halten
- ☐ Datenschutz-Hinweise für Patienten erstellen und zur Kenntnis bringen
- ☐ Datenschutz-Einwilligung von Patienten einholen
- ☐ Datenschutzerklärung erstellen und auf Website laden
- ☐ Mitarbeiter regelmäßig schulen
- ☐ Mitarbeiter auf Datengeheimnis verpflichten
- ☐ Auftragsverarbeitungsverträge mit Drittanbietern schließen
- ☐ Übersicht über technische und organisatorische Maßnahmen erstellen und aktuell halten
- ☐ ggf. Datenschutz-Folgenabschätzung vornehmen

Auf den folgenden Seiten erklären wir Ihnen jede einzelne dieser Aufgaben.

Falls Sie Nachfragen haben, kontaktieren Sie uns gerne unter **anfragen@heydata.eu** oder **+49 89 41325320**

#1 Verarbeitungsverzeichnis erstellen

Alle Arztpraxen müssen ein Verarbeitungsverzeichnis (VVZ) führen. Das VVZ gibt einen Überblick über alle Tätigkeiten, bei denen Arztpraxen mit personenbezogenen Daten umgehen. Diese Tätigkeiten sind z.B. der Einsatz eines Praxisverwaltungssytems oder das Führen von Personalakten.

Die bloße Auflistung aller Tätigkeiten reicht aber nicht. Für jede Tätigkeit sind zusätzlich u.a. die verarbeiteten Kategorien von Daten (z.B. Name, Adresse, Informationen zu durchgeführten Behandlungen), die Empfänger der Daten (z.B. andere Ärzte oder die Kassenärztliche Vereinigung) und die Aufbewahrungsfristen zu notieren. Ein richtig geführtes VVZ hat deshalb nicht zwei, sondern 10 Seiten und mehr.

Übrigens ist das VVZ meist das Dokument, das sich Datenschutzbehörden bei Überprüfungen als Erstes vorlegen lassen. Hier sauber zu dokumentieren, zahlt sich also aus.

Natürlich reicht es nicht, das VVZ ein einziges Mal aufzusetzen. Vielmehr bedarf das VVZ der regelmäßigen und vollständigen Aktualisierung. Ein Datenschutzbeauftragter von heyData kümmert sich für Sie um das VVZ, damit Sie sich ganz auf die Behandlung Ihrer Patienten konzentrieren können.

#2 Datenschutz-Hinweise für Patienten

Natürliche Personen haben ein Recht darauf, über die Verarbeitung ihrer personenbezogenen Daten informiert zu werden. Patienten bilden dabei keine Ausnahme. Sie sind vor oder bei Beginn des Behandlung umfassend zu informieren.

Die Hinweise müssen ähnliche Informationen wie das VVZ enthalten, gehen darüber aber noch hinaus. Auch Rechtsgrundlagen der Verarbeitung (z.B. aus dem Behandlungsvertrag) sind zu nennen und Informationen zu Betroffenenrechte hinzuzufügen.

Patienten müssen die Hinweise nicht formell akzeptieren. Arztpraxen sind aber verpflichtet, die Hinweise Patienten zur Kenntnis zu bringen. Ihr Datenschutzbeauftragter von heyData erstellt die Datenschutz-Hinweise für Sie und berät Sie, wie Sie Patienten die Informationen am einfachsten zur Verfügung stellen.

#3 Datenschutz-Einwilligung von Patienten

In vielen Fällen reichen bloße Datenschutz-Hinweise an Patienten aber nicht aus. Das ist immer dann der Fall, wenn eine Arztpraxis **Daten von Patienten an Dritte weitergibt** und dafür keine Übermittlungsverpflichtung oder -befugnis existiert.

Hier ist große Vorsicht geboten! Es gibt in dieser Frage einen Katalog an behördlicher und gerichtlicher Spruchpraxis, den es zu berücksichtigen gilt und der Änderungen unterworfen ist. Hier kann man leicht den Überblick verlieren.

Die wichtigsten Fälle der Weitergabe von Daten in Arztpraxen sind

- **Überweisung**: ohne Einwilligung
- Informationsaustausch zwischen Haus- an Facharzt: mit Einwilligung
- Krankenhauseinweisung: ohne Einwilligung
- Labor: ohne Einwilligung
- Rezeptübermittlung an Apotheken: mit Einwilligung
- **Übermittlung von Daten an die Kassenärztliche Vereinigung**: ohne Einwilligung

Besonders umstritten ist die Frage, ob die Übermittlung von Daten an private Abrechnungsstellen eine Einwilligung voraussetzt. Das wurde jedenfalls bis 2020 so angenommen. Mittlerweile ist die allgemeine Auffassung hier aber im Fluss. Natürlich halten wir von heyData Sie auch in dieser Frage informiert, damit Ihre Praxis stets datenschutzkonform handelt.

#4 Datenschutzerklärung für die Website

Dieselben Pflichten wie für die Verarbeitung von Patientendaten offline gelten auch für die Website online. In der **Datenschutzerklärung der Website** ist deshalb detailliert zu beschreiben, in welchem Umfang Ihre Arztpraxis **Daten über die Website verarbeitet**.

Verfügt Ihre Website über ein Kontaktformular? Können sich Interessenten auf Ihrer Website für einen Newsletter mit Praxis- oder Fachupdates registrieren? Oder suchen Sie personelle Verstärkung und veröffentlichen deshalb Stellenanzeigen auf Ihrer Website? All das sind Punkte, die in die Datenschutzerklärung gehören.

Besondere Beachtung müssen Arztpraxen **Angeboten von Drittanbietern** schenken, die sie in Ihre Website einbauen. Solche Werkzeuge können sehr hilfreich sein, um z.B. wie **Google Analytics** das Nutzungsverhalten der Seitenbesucher zu messen. Arztpraxen müssen in der Datenschutzerklärung aber auch ganz genau über die damit verbundene **Datenweitergabe** informieren.

In den meisten Fällen setzt die Weitergabe an Drittanbieter eine **ausdrückliche Einwilligung der Seitenbesucher** voraus. Ohne Cookie-Banner lässt sich dieser Einwilligung nicht einholen. Ihr Datenschutzbeauftragter berät Sie, wie Sie das Cookie-Banner richtig gestalten.

Ein zusätzliches Problem ist, dass viele **Drittanbieter in den USA** sitzen. Nach geltendem Recht ist aber eine Weitergabe von Daten in die USA nur sehr eingeschränkt möglich. Die Datenschutzbehörden prüfen sehr genau, ob datenverarbeitende Stellen sich an diese Vorgaben halten.

Lassen Sie sich unbedingt von Ihrem Datenschutzbeauftragten beraten, bevor sie Daten an Anbieter in den USA weitergeben! Ihr Datenschutzbeauftragter von heyData kennt sich mit dem Thema aus und erstellt für Sie die Datenschutzerklärung.

#5 Mitarbeiter

Die meisten Datenschutzpannen sind auf menschliches Versagen zurückzuführen. Wenn Sie Ihre Mitarbeiter mit den Grundlagen des Datenschutzes vertraut machen, können diese wie Schutzschilder Gefahren abwehren, statt **Datenschutzpannen** zu verursachen.

Eine regelmäßige Schulung Ihrer Mitarbeiter zahlt sich nicht nur aus, weil Sie Schäden durch Datenschutzpannen vermeiden, sondern auch weil sonst **kostspielige Bußgelder** drohen. Aus Sicht der Datenschutzbehörden ist eine regelmäßige Schulung Pflicht.

Die **Schulung Ihrer Mitarbeiter** gehört zu den Aufgaben Ihres Datenschutzbeauftragten. heyData hat viel Erfahrung, in der Schulung von Mitarbeitern. Wir wissen, worauf es ankommt und wie Mitarbeiter am meisten aus den Schulungen mitnehmen können.

Um sich haftungsrechtlich abzusichern, sollten Sie Ihre Mitarbeiter zusätzlich auf die Einhaltung der Datenschutzgesetze verpflichten. Und erlauben Sie Ihren Mitarbeitern, die Computer der Praxis zum privaten Surfen im Internet oder das E-Mail-Konto der Praxis zum Versenden privater E-Mails zu verwenden, ist eine Vereinbarung dazu ein Muss.

Ihr Datenschutzbeauftragter von heyData stellt Ihnen alle notwendigen Unterlagen zur Verfügung und aktualisiert sie, wenn dies durch Änderungen des Gesetzes erforderlich wird. Wenn Sie das Thema Datenschutz in professionelle Hände geben, können Sie sich einfach auf Ihre Patienten konzentrieren.

#6 Auftragsverarbeitungsverträge mit Drittanbietern

Erhalten andere Unternehmen Zugriff auf personenbezogene Daten einer Arztpraxis, ist Vorsicht geboten. Sie sind sogenannte Auftragsverarbeiter. Das kann z.B. auf IT-Unternehmen zutreffen, die Systeme eines Arztpraxens warten. Aber auch Anbieter von Software zur Terminbuchung fallen darunter.

Mit Auftragsverarbeitern müssen Arztpraxen spezielle Datenschutzverträge schließen. Diese **Auftragsverarbeitungsverträge** regeln, wie die externen Unternehmen mit den Daten umgehen und wie sie sie schützen. Trotz Auftragsverarbeitungsvertrags sind Arztpraxen aber dafür verantwortlich, ob die konkrete Verarbeitung zulässig ist - oder nicht.

Wenn Arztpraxen externen Unternehmen Zugriff auf personenbezogene Daten geben, ohne einen solchen Vertrag abzuschließen, riskieren sie ein Bußgeld. Ihr **Datenschutzbeauftragter von heyData** weiß, in welchen Situationen ein Auftragsverarbeitungsvertrag Pflicht ist und regelt für Sie den Vertragsschluss.

#7 Technische und organisatorische Maßnahmen

Ein weiteres Pflichtdokument für jede Arztpraxis ist eine **Übersicht über die technischen und organisatorischen Maßnahmen**. Darunter sind alle Schutzmaßnahmen zu verstehen, mit denen Arztpraxen personenbezogene Daten schützen.

In Betracht kommen viele Maßnahmen - von A wie einer Anweisung an Ihre Mitarbeiter, den Zugriff des Desktop-Computers zu sperren, wenn sie den Empfang verlassen, bis Z wie einer zentralen Verwaltung von Benutzerrechten für Ihre Systeme.

Die von einer Arztpraxis getroffenen Maßnahmen müssen im Verhältnis zu den betroffenen Daten stehen. Sind darunter Gesundheitsdaten, sind hohe Schutzmaßnahmen anzulegen. Über die konkret notwendigen Maßnahmen berät Sie gern Ihr Datenschutzbeauftragter von heyData. Außerdem kennt er alle technischen Fachbegriffe und erstellt für Sie das erforderliche Übersichtsdokument.

#8 Datenschutz-Folgenabschätzung

Für große Arztpraxen kann die Durchführung einer Datenschutz-Folgenabschätzung (DSFA) erforderlich sein. Im Rahmen einer DSFA werden die **Folgen einer konkreten und besonders risikoreiche Datenverarbeitung bewertet** und gegebenenfalls weitere Schutzmaßnahmen vorgeschlagen.

Aus Sicht der Datenschutzbehörden erfordert die Verarbeitung von Gesundheitsdaten in der Praxis eines alleine praktizierenden Arztes keine DSFA. Anders aber häufig in Gemeinschaftspraxen und MVZs: Ab einer Tätigkeit von vier Ärzten spricht viel dafür, dass der Umfang der Verarbeitung von Gesundheitsdaten eine DSFA notwendig macht.

Seien Sie hier bitte besonders aufmerksam! Die Durchführung einer DSFA ist kein leichtes Projekt. Sie erfordert eine genaue Prüfung und Bewertung möglicher Risiken. Sie ist keine Aufgabe, die ohne fachmännische Datenschutzberatung durchgeführt werden kann. Lassen Sie sich von Ihrem Datenschutzbeauftragten von heyData gerne beraten.

Selbst die Vorentscheidung, ob eine DSFA erforderlich ist, ist eine Fachfrage. Diese Entscheidung ist gut zu dokumentieren - und zwar für jede Verarbeitungstätigkeit! Mit Ihrem **Datenschutzbeauftragten von heyData** ist das kein Problem. Er unterstützt sie auch, wenn für Ihre Praxis eine DSFA durchzuführen ist, so dass für Sie so gut wie kein Aufwand entsteht.

Haben Sie weitere Fragen zu diesem Papier oder allgemein zum Datenschutz?

Unsere Experten prüfen Ihre Praxis gern in einem unverbindlichen Beratungsgespräch auf Datenschutzlücken.

Im Vertrieb
Miloš Djurdjević
Geschäftsführer
milos@heydata.eu

Ihr Datenschutzberater
Rechtsanwalt Martin Bastius
Chief Legal Officer
support@heydata.eu