KBV Kassenärztliche Bundesvereinigung
Körperschaft des öffentlichen Rechts

Ab 25. Mai gelten neue Vorschriften beim Datenschutz: Was Praxen jetzt tun müssen

Mit Stichtag 25. Mai 2018 gilt die neue Datenschutz-Grundverordnung der Europäischen Union. Ihre inhaltlichen Anforderungen ähneln vielfach dem derzeit geltenden Recht. Gleichwohl bringt sie zusätzliche Pflichten auch für Praxen mit sich. Zudem drohen bei Verstößen gegen die Vorgaben des Datenschutzes deutlich härtere Sanktionen. Was niedergelassene Ärzte und Psychotherapeuten jetzt tun müssen, stellt diese Praxisinformation vor.

Datenschutz wird noch wichtiger

Einhaltung des Datenschutzes muss nachgewiesen werden

Schon jetzt müssen Ärzte und Psychotherapeuten den Datenschutz wahren: gesetzliche Grundlagen sind insbesondere das SGB V und das Bundesdatenschutzgesetz. Nach der Datenschutz-Grundverordnung (DSGVO) sind sie künftig auch verpflichtet nachzuweisen, dass sie die datenschutzrechtlichen Grundsätze einhalten, zum Beispiel gegenüber den Aufsichtsbehörden. Außerdem kommen neue Informationspflichten gegenüber den Patienten hinzu.

DSGVO gilt nicht nur für Praxen

Die DSGVO gilt für den gesamten öffentlichen Bereich, also für private Unternehmen, öffentliche Stellen, freiberuflich Tätige oder Vereine. Sie vereinheitlicht die Regeln zur Verarbeitung personenbezogener Daten.

Um diese Daten und ihren Schutz geht es

Was die „Verarbeitung“ von Daten alles umfasst

Unter dem Begriff „Verarbeiten“ werden alle Tätigkeiten zusammengefasst wie Erheben und Abfragen, Ordnen, Speichern, Anpassen und Ändern, Auslesen und Weiterleiten, Löschen und Vernichten der Daten. In den Praxen beginnt dieser Prozess quasi bei der Terminvereinbarung am Telefon oder dem Einlesen der elektronischen Gesundheitskarte (eGK).

Es geht um personenbezogene Daten

Für Praxen geht es insbesondere um den Schutz der:

- Patientendaten (Gesundheitsdaten), die sie für die Behandlung der Patienten – ob gesetzlich oder privat versichert – benötigen, zum Beispiel Name und Versicherungsnummer, Befunde, Blutwerte, Röntgenaufnahmen
- Personaldaten, die sie als Arbeitgeber von ihren Mitarbeitern benötigen – zum Beispiel Name, Adresse, Sozialversicherungsnummer

Rein private Daten des Praxisinhabers, zum Beispiel die auf seinem Rechner gespeicherten Kontaktdaten von Familie und Freunden, unterliegen nicht der Datenschutz-Grundverordnung.

AUF EINEN BLICK: DAS IST IN PUNCTO DATENSCHUTZ JETZT ZU TUN

Viele Praxen haben längst Vorkehrungen getroffen und die Einhaltung des Datenschutzes zur „Chefsache“ erklärt. Jetzt geht es vor allem darum, die getroffenen Maßnahmen zu überprüfen und dafür zu sorgen, dass das Getane in puncto Datenschutz ab 25. Mai auch belegt werden kann. So können sie drohende Sanktionen vermeiden.

Die folgende Übersicht soll dabei helfen. Sie führt auf, was Praxen und Medizinische Versorgungszentren (MVZ) vorhalten müssen, um der Informations- und Nachweispflicht nach der DSGVO gerecht zu werden. Auf den nachfolgenden Seiten werden die Punkte näher erläutert. Nicht alles ist neu, sodass vorhandene Dokumente teilweise nur angepasst werden müssen.

Nicht alle Praxen benötigen alles

Übersicht

Was Praxen und MVZ ab 25. Mai benötigen

Alle:

- Verzeichnis von Verarbeitungstätigkeiten, das die Praxis auf Verlangen der Aufsichtsbehörde vorlegen kann
- Aufstellung der technischen und organisatorischen Maßnahmen, die die Praxis zum Schutz von personenbezogenen Daten ergreift
- Patienteninformation zum Datenschutz in der Praxis
- Vereinbarung zur Auftragsverarbeitung mit Softwareanbietern und anderen Dienstleistern, wenn diese auf Patienten- oder Mitarbeiterdaten zugreifen können

Große Praxen und große MVZ:

- Einen internen oder externen Datenschutzbeauftragten, wenn in der Praxis mindestens zehn Personen regelmäßig personenbezogene Daten automatisiert verarbeiten, zum Beispiel am Empfang

Darüber hinaus kann dies erforderlich sein:

- In seltenen Fällen kann eine Datenschutz-Folgenabschätzung nötig sein, zum Beispiel wenn große Mengen an personenbezogenen Daten verarbeitet oder die Praxisräume systematisch videoüberwacht werden. Diese Praxen benötigen unabhängig von der Anzahl der Mitarbeiter ebenfalls einen Datenschutzbeauftragten.
- Praxen, die mit Einwilligungserklärungen des Patienten arbeiten, zum Beispiel bei der Weitergabe von Daten an eine privatärztliche Verrechnungsstelle, müssen die Erklärung um einen Hinweis auf Widerrufbarkeit ergänzen.
- Praxen, die eine Internet- oder Facebook-Seite anbieten, sollten die Datenschutzerklärung prüfen und gegebenenfalls anpassen; dies gilt ebenso, wenn personenbezogene Daten zum Beispiel über Kontaktformulare oder für einen Praxis-Newsletter erfasst und gespeichert werden.

TIPP: Nutzen Sie die Checkliste „Das ist in puncto Datenschutz zu tun“: www.kbv.de/datenschutz

Checkliste im Internet

HINWEISE UND EMPFEHLUNGEN ZUR UMSETZUNG

Was Praxen und MVZ ab 25. Mai benötigen – auf den folgenden Seiten werden die einzelnen Punkte näher erläutert. Zudem gibt es Hinweise auf Muster und weiterführende Informationen, die die KBV im Internet bereitstellt.

Die Details

Verzeichnis von Verarbeitungstätigkeiten

Verzeichnis muss Aufsichtsbehörde auf Verlangen vorgelegt werden

Praxen benötigen ein Verzeichnis von Verarbeitungstätigkeiten. Darin werden Tätigkeiten beziehungsweise Vorgänge erfasst, bei denen in der Praxis personenbezogene Daten verarbeitet werden. Die Aufstellung und Beschreibung der Tätigkeiten ist auf Verlangen der Aufsichtsbehörde bereitzustellen. Liegt kein Verzeichnis vor, drohen Geldstrafen.

Das ist zu tun

Muster mit Beispielen

Die KBV stellt für das Verzeichnis ein Muster bereit, das Sie nutzen können. Dazu gibt es ein Ausfüllbeispiel mit zwei Verarbeitungstätigkeiten. So können Sie vorgehen:

Tätigkeiten, bei denen Daten verarbeitet werden, zusammenstellen

Schritt 1: Für das Erstellen des Verzeichnisses sollten Sie zunächst überlegen, wo überall in der Praxis personenbezogene Daten verarbeitet, also zum Beispiel erhoben, gespeichert, bearbeitet oder weitergeleitet, werden. Dabei bietet es sich an, Tätigkeiten, die demselben Zweck dienen, zusammenzufassen.

Eine Tätigkeit, die in allen Praxen anfallen dürfte, ist die Nutzung des Praxisverwaltungssystems zum Zwecke der ärztlichen / psychotherapeutischen Dokumentation in der Patientenakte, der Qualitätssicherung, der Terminplanung und der Abrechnung. Eine weitere Tätigkeit ist beispielsweise das Führen von Personalakten, um Mitarbeiter beschäftigen zu können.

Angaben zu den Tätigkeiten

Schritt 2: Im nächsten Schritt fügen Sie zu jeder Tätigkeit die in der DSGVO geforderten Angaben hinzu. Das sind:

- Zweck der Verarbeitung (z.B. ärztliche Dokumentation)
- betroffene Personengruppen (z.B. Patienten, Beschäftigte)
- Datenkategorien (z.B. Gesundheitsdaten, Personaldaten)
- Empfängergruppen, gegenüber denen die personenbezogenen Daten offengelegt werden (z.B. Krankenkassen, Kassenärztliche Vereinigungen)
- Fristen für die Löschung (z.B. zehn Jahre)

Angaben zur Praxis

Schritt 3: Geben Sie jetzt noch den Namen und die Kontaktdaten Ihrer Praxis und gegebenenfalls des Datenschutzbeauftragten an. Dazu füllen Sie die Felder auf der ersten Seite der Dokumentenvorlage aus.

Prüfen Sie bei der Erstellung des Verzeichnisses auch, ob bestimmte Datenverarbeitungsvorgänge ein besonders hohes Risiko bergen. Dann könnte unter Umständen eine Datenschutz-Folgenabschätzung nötig sein (s. S. 7).

TIPP: Das Muster für ein Verarbeitungsverzeichnis und das Ausfüllbeispiel finden Sie hier: www.kbv.de/datenschutz

Aufstellung der Maßnahmen zum Datenschutz

Interne Regeln zum Umgang mit sensiblen Daten

Praxen sind für den Schutz personenbezogener Daten verantwortlich. Sie müssen dazu geeignete technische und organisatorische Maßnahmen ergreifen und diese dokumentieren. So kennen alle Teammitglieder die Regeln, und bei externen Kontrollen oder Anfragen kann der interne Datenschutzplan vorgelegt werden.

Diese Maßnahmen zum Datenschutz gehören dazu

Die DSGVO macht keine konkreten Vorgaben, welche Maßnahmen im Einzelnen dokumentiert werden soll. Doch letztlich geht es darum, zu erfassen, welche Vorkehrungen die Praxis getroffen hat, um einen Missbrauch von personenbezogenen Daten zu verhindern. Auf diese Punkte kommt es insbesondere an:

Maßnahmen zum Datenschutz in der Praxis

- Patientendaten werden niemals unverschlüsselt über das Internet versendet, beispielsweise per E-Mail.
- Zugriffsberechtigungen sind vergeben; somit ist klar geregelt, wer in der Praxis auf Dateien und Ordner zugreifen kann.
- In den Praxisräumlichkeiten wird auf Diskretion geachtet: Die Anmeldung sollte getrennt zum Wartebereich angeordnet sein. Möglich ist auch, Patienten beispielsweise mit einem Schild darauf hinzuweisen, dass sie am Tresen Abstand halten sollen, wenn mehrere Personen dort warten.
- Patientenakten werden sicher verwahrt: Die Computer sind passwortgeschützt, die automatische Bildschirmsperre ist aktiviert. Patientenunterlagen werden stets so positioniert, dass andere Patienten diese nicht einsehen können. Wenn der Arzt / Psychotherapeut nicht im Raum ist, werden Patientenakten generell unter Verschluss gehalten.
- Vertrauliche Arzt-Patienten-Gespräche finden stets in geschlossenen Räumen statt.
- Bei Auskünften am Telefon wird die Identität des Anrufers gesichert, zum Beispiel durch gezielte Zusatzfragen oder einen Rückruf.
- Es ist festgelegt, wann und durch wen personenbezogene Daten gelöscht beziehungsweise vernichtet werden, sobald beispielsweise die Aufbewahrungsfrist abläuft.
- Patientenakten werden nach DIN-Normen vernichtet.
- Es ist festgelegt, was bei Datenpannen und Datenschutzverstößen zu tun ist und wer die Meldung übernimmt (in der Regel an die zuständige Aufsichtsbehörde innerhalb von 72 Stunden).
- Die Mitarbeiter in der Praxis wurden über die Einhaltung von Schweigepflicht und Datenschutz informiert.

Patienteninformation zum Datenschutz in der Praxis

Praxen müssen Patienten darüber informieren, was mit ihren Daten passiert. Dies muss in der Regel zum Zeitpunkt der Datenerhebung erfolgen.

Patienten müssen über Umgang mit ihren Daten informiert werden

Die Information muss in erster Linie Angaben zum Zweck sowie zur Rechtsgrundlage der Datenverarbeitung enthalten. Auch die Kontaktdaten der Praxis und gegebenenfalls des Datenschutzbeauftragten sind aufzuführen.

Das ist zu tun

Um alle Patienten zu erreichen, empfiehlt sich ein Aushang in der Praxis. Auch ein Informationsblatt, das im Wartezimmer ausgelegt wird, ist möglich. Die Patienteninformation kann zusätzlich auf der Website der Praxis veröffentlicht werden. Eine persönliche Information, zum Beispiel bei der ersten Kontaktaufnahme am Telefon, ist nicht erforderlich.

Aushang in der Praxis, Information im Internet

TIPP: Die KBV stellt ein Muster für eine Patienteninformation bereit: www.kbv.de/datenschutz

Muster für Patienteninformation

Auftragsverarbeitung: Zusammenarbeit mit Dienstleistern

Die Praxissoftware wird gewartet, Akten- und Datenträger müssen nach Ablauf der Aufbewahrungsfrist vernichtet werden. Immer dann, wenn ein externer Dienstleister auf Patienten- oder Mitarbeiterdaten zugreifen kann, ist der Abschluss eines Vertrages zur Auftragsverarbeitung (als Anlage zum Hauptvertrag) erforderlich.

Die Auftraggeber müssen sich ferner davon überzeugen, dass der Dienstleister die Vorschriften des Datenschutzes einhält und entsprechende technische und organisatorische Maßnahmen durchführt. Die Firmen sollen dem Auftragsnehmer dazu ein Datenschutzsiegel oder eine Zertifizierung, zum Beispiel ISO/IEC 27001, vorlegen.

Auftragsverarbeitung: ja oder nein?

Eine Auftragsverarbeitung liegt nicht nur bei der Wartung der Praxis-EDV oder der Akten- und Datenträgervernichtung vor. Weitere Beispiele sind die Nutzung von Cloud-Systemen und die Terminvergabe durch Externe (die Terminservicestellen der KVen fallen nicht darunter). Dagegen ist eine rein technische Wartung der IT-Infrastruktur durch einen Externen, zum Beispiel Arbeiten an der Stromzufuhr, Kühlung oder Heizung, keine Auftragsverarbeitung. Dies gilt ebenso bei der Beauftragung von Steuerberatern, Rechtsanwälten, Wirtschaftsprüfern und Angehörigen anderer Berufe, die als „Geheimnisträger“ gelten. Auch hier liegt in der Regel keine Auftragsverarbeitung vor.

Beispiel für Auftragsverarbeitung

Das ist zu tun

Schritt 1: Schauen Sie zunächst, ob Sie für Ihre Dienstleistungsverträge (z.B. zur Wartung der Praxis-EDV) jeweils einen Vertrag zur Auftragsverarbeitung haben, und passen Sie diesen in Abstimmung mit dem Auftragnehmer gegebenenfalls an.

Vertrag zur Auftragsverarbeitung abschließen

Schritt 2: Ist das nicht der Fall, sprechen Sie Ihren Dienstleister an. Er benötigt einen Vertrag zur Auftragsverarbeitung und wird Ihnen in der Regel einen Entwurf zusenden.

Das sollte der Vertrag enthalten

Folgende Inhalte sollte der Vertrag enthalten:

- Gegenstand und Dauer der Verarbeitung (um welche Leistung handelt es sich, wie lange wird diese beauftragt)
- Art und Zweck der Verarbeitung (wozu dient sie, welches Ziel soll erreicht werden)
- Art der personenbezogenen Daten und Kategorien betroffener Personen (z.B. Zugriff auf Gesundheitsdaten)
- Rechte und Pflichten des Auftraggebers sowie dessen Weisungsbefugnisse
- Verpflichtung der zur Verarbeitung berechtigten Personen zur Vertraulichkeit
- Benennung der technischen und organisatorischen Maßnahmen, die das Unternehmen zum Schutz personenbezogener Daten durchführt (z.B. Einhaltung von Vorgaben der ISO/IEC 27001)
- Verpflichtung des Auftragnehmers zur Unterstützung des Auftraggebers bei:
    - Anfragen und Ansprüchen Betroffener im Zusammenhang mit der Auftragsverarbeitung
    - der Meldepflicht bei Datenschutzverletzungen und der Datenschutz-Folgenabschätzung
- Rückgabe oder Löschung personenbezogener Daten nach Abschluss der Auftragsverarbeitung
- Verpflichtung des Auftragnehmers, dem Auftraggeber alle Informationen zum Nachweis der Einhaltung der datenschutzrechtlichen Pflichten bereitzustellen. Möglich ist auch eine Überprüfung oder Inspektion durch einen vereinbarten Prüfer.

Nachweis des Auftragnehmers zur Einhaltung des Datenschutzes

Schritt 3: Lassen Sie sich vom Dienstleister ein geeignetes Zertifikat, zum Beispiel ISO/IEC 27001, vorlegen. Das Zertifikat dient dem Nachweis der eingesetzten technischen und organisatorischen Maßnahmen zum Schutz der Daten beim Auftragnehmer. Eine weitergehende Pflicht zur Kontrolle durch Sie besteht nicht.

Datenschutzbeauftragten benennen – ab zehn Personen

Pflicht auch bei Datenschutz-Folgenabschätzung

Größere Praxen und MVZ benötigen einen Datenschutzbeauftragten. Wie bisher ist dies Pflicht, wenn mindestens zehn Personen regelmäßig Daten automatisiert – zum Beispiel am Computer – verarbeiten. In seltenen Fällen müssen auch kleinere Praxen einen Datenschutzbeauftragten einsetzen, nämlich wenn eine Datenschutz-Folgenabschätzung notwendig wird (s. S.7).

Mitteilung an Landesdatenschutzbeauftragten

Die Aufgabe des Datenschutzbeauftragten kann ein fachlich qualifizierter Mitarbeiter (nicht der Praxisinhaber) oder ein externer Datenschützer übernehmen. Name und Kontaktdaten des Datenschutzbeauftragten müssen dem Landesdatenschutzbeauftragten mitgeteilt werden.

Aufgabe des Datenschutzbeauftragten ist es, die Einhaltung des Datenschutzes und der Datensicherheit in der Praxis zu kontrollieren und geeignete Maßnahmen festzulegen. Er informiert und berät das Praxisteam über ihre Pflichten nach dem Datenschutzrecht. Darüber hinaus ist er Ansprechpartner für die Aufsichtsbehörde.

Aufgaben des Datenschutzbeauftragten

Datenschutz-Folgenabschätzung

In seltenen Fällen kann eine Datenschutz-Folgenabschätzung erforderlich sein, zum Beispiel wenn aufgrund des Umfangs und des Zwecks der Datenverarbeitung ein hohes Datenschutzrisiko besteht. Auch eine systematische Videoüberwachung der Praxisräume kann ein Grund sein.

Nur selten erforderlich

Bestehen möglicherweise hohe Risiken bei der Datenverarbeitung, ist eine externe Datenschutzprüfung zu empfehlen. Sollten Sie Zweifel haben, ob dies im Einzelfall nötig ist, empfiehlt es sich, dies beim Landesdatenschutzbeauftragten zu erfragen.

Ist eine Datenschutz-Folgenabschätzung erforderlich, muss ein Datenschutzbeauftragter benannt werden, auch wenn in der Praxis weniger als zehn Mitarbeiter tätig sind.

Einwilligungserklärungen anpassen

Das Erfassen, Bearbeiten, Speichern etc. von Patientendaten ist gesetzlich gestattet. Nur in besonderen Fällen kann es erforderlich sein, dass Patienten zustimmen müssen, zum Beispiel bei der Einbeziehung einer privatärztlichen Verrechnungsstelle. In diesen Fällen müssen Praxen nachweisen können, dass die Patienten eine Einwilligungserklärung zur Datenverarbeitung unterschrieben haben.

Das ist zu tun

Ab 25. Mai müssen Einwilligungserklärungen einen Hinweis darauf enthalten, dass Patienten ihr Einverständnis jederzeit widerrufen können. Ergänzen Sie gegebenenfalls Ihre Vorlagen.

Erklärung muss Hinweis auf Widerruf enthalten

Datenschutzerklärung auf der Internetseite

Zahlreiche Praxen haben eine Internet- oder Facebook-Seite. Terminerinnerungen per SMS oder Patienten-Newsletter gehören zunehmend zum Serviceangebot. Auch dabei werden personenbezogene Daten verarbeitet, die geschützt werden müssen.

Das ist zu tun

Prüfen Sie, ob auf Ihrer Internet- oder Facebook-Seite eine Datenschutzerklärung eingestellt ist und diese alle nötigen Angaben beinhaltet. Außerdem können Sie die Patienteninformation zum Datenschutz in der Praxis auf Ihre Internetseite stellen.

Hinweise zum Datenschutz auf der Praxis-Website

Weisen Sie in der Datenschutzerklärung unter anderem darauf hin, dass

- personenbezogene Daten wie Name, Postanschrift, E-Mail-Adresse, Telefonnummer oder das Geburtsdatum ausschließlich in Übereinstimmung mit dem jeweils geltenden Datenschutzrecht erhoben und genutzt werden

- die Daten nur gespeichert werden, wenn sie aktiv übermittelt werden
- die Daten zum Beispiel nur zur Beantwortung von Anfragen oder zur Zusendung von Informationsmaterial verwendet werden
- Kontaktdaten, die im Rahmen von Anfragen angegeben werden, ausschließlich für die Korrespondenz verwendet werden
- E-Mail-Adressen, die Nutzer für den Bezug eines Newsletters angegeben haben, nur dafür genutzt werden

Bei Verstößen drohen hohe Geldstrafen

Das Ausmaß der Sanktionen richtet sich vor allem nach der Schwere und der Dauer des Vorfalls sowie nach dessen Auswirkungen auf die Patienten. Leichte Verstöße werden zunächst zu einer Beratung führen.

Dennoch sollten Praxen alle nötigen Vorkehrungen treffen. Denn die DSGVO sieht bei Verstößen generell deutlich härtere Sanktionen vor als sie bisher üblich sind. Die Aufsichtsbehörden – in der Regel die Landesdatenschutzbeauftragten – können im Einzelfall Geldbußen von bis zu 20 Millionen Euro verhängen. Liegt kein Verzeichnis von Verarbeitungstätigkeiten vor, können bis zu zehn Millionen Euro oder bis zu zwei Prozent des Jahresumsatzes verlangt werden. Möglich sind zudem Schadensersatzforderungen von Betroffenen inklusive Schmerzensgeld, zum Beispiel wegen Rufverletzung.

Hohen Geldbußen und Schadensersatzforderungen

Mehr Informationen

KBV-Themenseite Datenschutz mit allen Informationen zur Datenschutz-Grundverordnung, Checklisten und Muster, zum Beispiel für eine Patienteninformation: www.kbv.de/datenschutz

Weitere Infos im Internet

Kennen Sie schon die PraxisNachrichten? Sie können den Newsletter der KBV hier kostenlos abrufen und abonnieren: www.kbv.de/praxisnachrichten.