Leitfaden Datenschutz in der Zahnarztpraxis

Gesamtinhalt

* Die unter dem Registerblatt „CD-ROM" aufgeführten Checklisten und Mustervorlagen stehen Ihnen als Download zur Verfügung.

Inhalt Download

Checklisten und Mustervorlagen

Arbeitsanweisungen und Unterweisungen

Checklisten

Einverständniserklärungen

- Einwilligungserklärung zum Austausch von Patientendaten in der Praxisgemeinschaft
- Einwilligungserklärung für die Abrechnung über eine privatzahnärztliche Abrechnungsgesellschaft
- Schweigepflichtentbindungserklärung für die Weitergabe von Unterlagen an den weiterbehandelnden Zahnarzt
- Schweigepflichtentbindung für die Herausgabe von Unterlagen an Dritte

Merk- und Informationsblätter

- Datenschutzregelung in unserer Praxis
- Informationsformular für die betroffene Person über die Erhebung personenbezogener Daten
- Merkblatt – Patienteninformation zum Datenschutz
- Auszüge aus den Gesetzestexten als Begleitunterlagen zur Unterweisung
- Patienteninformation – PIN vergessen? So gehen Sie vor
- Patienteninformation zur ePA
- Kurzübersicht: Datenschutz in der ePA
- Kurzübersicht: ePA-Einwilligung beim Patienten einholen

Mustervorlagen und -formulare

- Patienteninformation
- Beispiel für eine praxisinterne IT-Richtlinie
- Bestellung zur/zum externen Datenschutzbeauftragten
- Datenschutzerklärung für die Webseite
- Fehlerliste Datenschutz – blanko
- Maßnahmenkatalog – ausgefüllt
- Maßnahmenkatalog – blanko
- Meldung bei Datenpannen an die Aufsichtsbehörde
- Meldung bei Datenpannen an die betroffenen Personen
- Technische und organisatorische Maßnahmen
- Verzeichnis von Verarbeitungstätigkeiten
- Vorlage – Zuständigkeiten und Verantwortlichkeiten mit Vertretungsregelung
- IT-Sicherheits-Handbuch

- Muster-Vorlage zum Ablauf einer Mitarbeiter-Datenschutzschulung mit Verständnisabfrage
- Meldeformular bei Datenpannen an die Aufsichtsbehörde
- Begrüßungsnachricht zur Messengernutzung für Ihre Datenschutzerklärung
- KI-Notfallkonzept
- Musteranschreiben – Meldung eines Datenschutzvorfalls (ePA)
- Meldeformular – Datenschutzvorfall (ePA)
- Arbeitsanweisung – Umgang mit der elektronischen Patientenakte (ePA)

Vereinbarungen

- Sicherheitsvereinbarung
- Vertraulichkeitsvereinbarung
- Mustervertrag zur Auftragsdatenverarbeitung
- Vollmacht für die Abholung von Rezepten, Befunden etc.

Checklisten und Vorlagen zur Telematik

- Vorab-Checkliste für Ihre Zahnarztpraxis
- Checkliste zur Anbindung an die Telematik
- Checkliste zur Antragsstellung SMC-B
- Checkliste zur Antragsstellung eZahnarztausweis
- FAQ – Häufig gestellte Fragen und Antworten

Fehlermeldungen

- Bedeutungen der Prüfnachweise
- Fehler beim Lesen der VSD mit Abbruch aufgrund von technischen Fehlern
- Fehler beim Lesen der VSD mit Abbruch durch ungültige eGK
- Fehlercodes und Fehlermeldungen

2 Patienten und Datenschutz

Was bedeutet Datenschutz?

Unter Datenschutz versteht man den Schutz personenbezogener Daten vor Missbrauch, oft auch im Zusammenhang mit dem Schutz der Privatsphäre. Zweck und Ziel des Datenschutzes ist die Sicherung des Grundrechts auf informationelle Selbstbestimmung der Einzelperson. Jeder soll selbst bestimmen können, wem er wann, welche seiner Daten und zu welchem Zweck zugänglich macht.

Patientendaten

Ein besonders sensibler Bereich ist dabei das Thema Patientendaten. Hier handelt es sich um Daten, die einen höchstpersönlichen Bereich betreffen. Gelangen diese Daten in die falschen Hände, kann dies unabsehbare Folgen haben. Deshalb genießen Patientendaten einen besonders hohen Schutz. Wer mit ihnen umgeht, ist also dem Datenschutz und dem Datengeheimnis besonders verpflichtet.

2.1 Rechtliche Grundlagen des Patientengeheimnisses

Standesrecht

Neben dem Datenschutzrecht ergibt sich auch aus verschiedenen anderen Rechtsbereichen eine besondere Verpflichtung derjenigen, die mit Patientendaten umgehen. So beinhaltet das Standesrecht in den Berufsordnungen der Ärzte- bzw. Zahnärztekammern, der Apothekenkammern und der Psychotherapeutenkammern, die Pflicht zur Dokumentation einer Behandlung, das Recht des Patienten auf Akteneinsicht, die Pflicht zur Verschwiegenheit, aber auch bestimmte Befugnisse zur Übermittlung von Patientendaten.

Bürgerliches Gesetzbuch (BGB)

Das Bürgerliche Gesetzbuch enthält eine ganze Fülle von Regelungen zu den Patientenrechten (§ 630a ff. BGB) und Bestimmungen, die ebenfalls den Bereich Patientendaten berühren. Die Behandlung des Patienten basiert auf einem von ihm gewünschten Behandlungsvertrag. Aus dem Schluss des Behandlungsvertrages ergeben sich u. a. wiederum Pflichten des Arztes/Zahnarztes zum Umgang mit Patientendaten. § 630f BGB verpflichtet den Arzt/Zahnarzt, wie bisher schon in den Berufsordnungen und dem Standesrecht festgelegt, eine Patientenakte zu führen und alle relevanten Fakten ausführlich zu dokumentieren:

„Der Behandelnde ist verpflichtet, in der Patientenakte sämtliche aus fachlicher Sicht für die derzeitige und künftige Behandlung we-

sentlichen Maßnahmen und deren Ergebnisse aufzuzeichnen, insbesondere die Anamnese, Diagnosen, Untersuchungen, Untersuchungsergebnisse, Befunde, Therapien und ihre Wirkungen, Eingriffe und ihre Wirkungen, Einwilligungen und Aufklärungen. Arztbriefe sind in die Patientenakte aufzunehmen."

Nachträgliche Änderungen

Nachträgliche Änderungen, sowohl in der auf Papier geführten Akte, als auch in der elektronischen Patientenakte, müssen den konkreten Inhalt und den genauen Zeitpunkt der Änderung erkennen lassen.

SGB V

Weitere Regelungen finden sich in besonderen Datenschutzregelungen der Krankenhausgesetze, der Sozialgesetzbücher (insbesondere SGB V) und einer Vielzahl weiterer spezifischer Gesetze, wie z. B. dem Infektionsschutzgesetz.

§ 203 StGB

Wichtig: Im Strafrecht stellt § 203 Strafgesetzbuch (StGB) die unbefugte Offenbarung von Patientendaten unter Strafe (Geldstrafe oder sogar bis zu zwei Jahre Gefängnis).

4.2 Datenschutzbeauftragter

Wann ist ein Datenschutzbeauftragter erforderlich?

Nach den neuen Regelungen der DSGVO stellt sich die weitreichende Frage, inwieweit die Zahnarztpraxis einen Datenschutzbeauftragten benötigt. Ob dies der Fall ist, hängt von den jeweiligen Gegebenheiten der betroffenen Praxis ab. Einschlägige Regelungen zur Benennung eines Datenschutzbeauftragten finden sich in Artikel 37 DSGVO.

Danach ist jedenfalls in drei aufgeführten Konstellationen ein Datenschutzbeauftragter zwingend erforderlich:

Voraussetzung für die Erfordernis eines Datenschutzbeauftragten

- Die Praxis ist Teil einer Behörde oder öffentlichen Stelle.
- Die Kerntätigkeit besteht in der Durchführung von Datenverarbeitungen, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche, regelmäßige und systematische Überwachung erforderlich macht.
- Die Kerntätigkeit besteht in der umfangreichen Verarbeitung von besonderen Kategorien von Daten im Sinne des Artikels 9 DSGVO (insbesondere Gesundheitsdaten).

Auch wenn eine Zahnarztpraxis theoretisch auch als öffentliche Stelle betrieben werden könnte, kann diese Konstellation hier vernachlässigt werden und ist nicht weiter zu betrachten.

Kerntätigkeit

Ein Datenschutzbeauftragter ist weiter dann zu benennen, wenn die Kerntätigkeit die Durchführung von Datenverarbeitungen betrifft. Auch wenn in der durchschnittlichen Zahnarztpraxis eine Menge von Daten erhoben und verarbeitet werden, ist die Datenverarbeitung jedoch nicht die Kerntätigkeit der Zahnarztpraxis. Die Datenverarbeitung ist vielmehr ein notwendiges „Nebenprodukt" des Betriebes der Zahnarztpraxis. Diese Variante des Artikels 37 DSGVO scheidet somit bei der durchschnittlichen Zahnarztpraxis ebenfalls aus. Es verbleibt damit das Kriterium des Artikels 37 Absatz 3 DSGVO. Danach ist ein Datenschutzbeauftragter zu benennen, wenn die Kerntätigkeit der Praxis in der umfangreichen Verarbeitung u. a. von Gesundheitsdaten besteht.

Wann liegt umfangreiche Datenverarbeitung vor?

Es stellt sich nun die Frage, wann eine „umfangreiche" Datenverarbeitung von Gesundheitsdaten vorliegt. Aus den Regelungen der DSGVO lässt sich dies nicht direkt beantworten. Hinweise, wie der Begriff auszulegen ist, finden sich insbesondere in den Erwägungsgründen der DSGVO.

Erwägungsgrund f. Datenschutz-Folgenabschätzung

Hier ist speziell auf Erwägungsgrund 91 zu verweisen, über den jedenfalls eine negative Abgrenzung erfolgen kann. Der Erwägungsgrund befasst sich mit der Frage, wann eine sogenannte Datenschutz-Folgenabschätzung vorzunehmen ist, nämlich bei „umfangreichen Verarbeitungsvorgängen". Am Ende des Erwägungsgrundes heißt es schließlich: *„Die Verarbeitung personenbezogener Daten sollte nicht als umfangreich gelten, wenn die Verarbeitung personenbezogene Daten von Patienten oder von Mandanten betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes oder Rechtsanwalt erfolgt. In diesen Fällen sollte eine Datenschutz-Folgenabschätzung nicht zwingend vorgeschrieben sein".*

Einzelpraxen

Wichtig: Daraus kann der Rückschluss gezogen werden, dass zumindest Einzelpraxen häufig nicht über einen Datenschutzbeauftragten verfügen müssen.

Datenschutzbeauftragter zwingend erforderlich

Im Umkehrschluss kann dann aber auch gesagt werden, dass Berufsausübungsgemeinschaften zwingend über einen Datenschutzbeauftragten verfügen müssen. Gleiches gilt danach ebenso für medizinische Versorgungszentren.

Datenschutzbeauftragter in Praxisgemeinschaften

Auch bei der Praxisgemeinschaft als Zusammenschluss mehrerer Zahnärzte wird man jedenfalls dann von einer „umfangreichen Datenverarbeitung" ausgehen müssen, wenn eine gemeinsame Datenverarbeitungs-Struktur genutzt wird, also die Patientendaten in einem gemeinsamen EDV-System zusammengeführt sind.

Ein weiteres Kriterium, wann ein Datenschutzbeauftragter zwingend zu bestellen ist, findet sich schließlich in § 38 BDSG-neu:

(1) Ergänzend zu Artikel 37 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679 benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Nehmen der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vor, die einer Datenschutz-Folgenabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 unterliegen, oder verarbeiten sie personenbezogene Daten geschäftsmäßig zum Zweck der Über-

mittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung, haben sie unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen.

(2) § 6 Absatz 4, 5 Satz 2 und Absatz 6 finden Anwendung, § 6 Absatz 4 jedoch nur, wenn die Benennung einer oder eines Datenschutzbeauftragten verpflichtend ist.

Datenschutzbeauftragte abhängig v. Betriebsgröße

Ein Datenschutzbeauftragter muss danach zwingend bestellt werden, wenn in der Zahnarztpraxis in der Regel mindestens zwanzig Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind oder in der Zahnarztpraxis Datenverarbeitungen vorgenommen werden, die einer Datenschutz-Folgenabschätzung im Sinne des Artikels 35 DSGVO unterliegen.

Da gemäß Erwägungsgrund 91 DSGVO eine Datenschutz-Folgenabschätzung bei Einzelpraxen häufig nicht erforderlich ist, kann zusammenfassend festgestellt werden, dass die Bestellung eines Datenschutzbeauftragten zwingend erforderlich ist:

- bei Praxen mit mindestens 20 Personen, die an der Datenverarbeitung beteiligt sind (einschließlich Praxisinhaber)
- bei Berufsausübungsgemeinschaften und MVZ
- bei Praxisgemeinschaften mit gemeinsam genutzter Datenverarbeitungs-Infrastruktur

Wichtig: § 38 BDSG ist durch das 2. Datenschutz-Anpassungs- und Umsetzungsgesetz EU (2. DSAnpUG-EU) vom 27.06.2019 geändert worden. Ursprünglich betrug die Anzahl der Personen, die ständig mit der Datenverarbeitung beschäftigt sein mussten, zehn. Mit der Änderung reagierte der Bundestag auf Kritik aus Wirtschaft und Verbänden, in der die Belastung gerade für kleine Unternehmer thematisiert worden war. Das Gesetz ist am 20.11.2019 in Kraft getreten, nachdem der Bundesrat der Änderung zugestimmt hatte. Damit ist seitdem die Zahl 20 verbindlich.

Zu beachten ist allerdings, dass davon unabhängig auch Betriebe, die nicht zwingend einen Datenschutzbeauftragten bestellen müssen, weil weniger als 20 Personen dort mit der Datenverarbeitung befasst sind, die Vorgaben der DSGVO ansonsten zu erfüllen haben, wie z. B. die Erstellung eines Verzeichnisses der Datenverarbeitungstätigkeiten etc. Gibt es keinen Datenschutzbeauftragten, liegt die Verpflichtung zum Einhalten des Datenschutzes weiterhin bei den sogenannten Verantwortlichen, also den Praxisinhabern. Es kann also gute Gründe geben, gleichwohl einen Datenschutzbeauftragten (extern oder intern) zu installieren oder zumindest einen externen Dienstleister zur Erfüllung der Aufgaben zu bestellen.

Ab 20 an Datenverarbeitung beteiligten Personen

Im Ergebnis bleibt festzuhalten, dass die Bestellung eines Datenschutzbeauftragten jedenfalls dann unumgänglich ist, wenn die Zahnarztpraxis einen erheblichen Umfang hat. Das ist insbesondere an der Zahl der beschäftigten Personen zu messen, die regelmäßig Datenverarbeitungsvorgänge in der Praxis durchführt. Liegt die Zahl über 20 Personen, wobei Praxisinhaber und Leitungspersonal mitgezählt werden müssen, wenn sie mit entsprechenden Tätigkeiten mindestens teilweise und nicht nur ganz untergeordnet befasst sind, besteht eine entsprechende Verpflichtung.

Eine individualisierbare Checkliste zur Benennung eines Datenschutzbeauftragten finden Sie auf beiliegender CD-ROM.

Weitere Anforderungen

Wichtig: Ist die Bestellung eines Datenschutzbeauftragten erforderlich, ergeben sich die weiteren Anforderungen an die zu bestellende Person aus Artikel 37 DSGVO.

Qualifikation

Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 39 DSVGO genannten Aufgaben.

3.6 Diskretion und Verschwiegenheit im Praxisalltag

Räumliche Umsetzung

Die räumliche Umsetzung des Datenschutzes und die damit verbundene Diskretion in Praxen sind mancherorts optimierungsfähig. Bei Praxisbegehungen kann die praktische Umsetzung der Datenschutzregeln zu Bemängelungen führen.

Praxisbeispiel

Sie kennen vielleicht folgende Situation am Empfang der Praxis: Die Mitarbeiterin spricht am Telefon mit einem Patienten Termine ab und beantwortet dessen Fragen. Ein Patient betritt die Praxis und steht am Empfang, um sich anzumelden. Im selben Moment kommt ein Behandler mit einem Patienten aus dem Behandlungszimmer. Da der Patient noch Fragen hat, beantwortet der Behandler diese am Empfang. Eine Kollegin ruft im Vorbeieilen: „Würdest Du bitte Frau Anika Meier anrufen. Die hat die letzten beiden Termine schon sausen lassen!". Die Tür des Wartezimmers ist offen, sodass die wartenden Patienten alle Gespräche mitverfolgen können. Der Patient, der am Empfang auf seine Anmeldung wartet, beobachtet das Szenario interessiert und denkt sich dabei: „Anika Meier?, Ach, hat die sich nicht bei mir als Auszubildende beworben?".

Bedenkliches Verhalten

Dieses Szenario lässt sich noch beliebig mit Beispielen ausweiten – denken Sie nur an Ihre eigenen Arztbesuche. Es steckt kein böser Wille dahinter, zumeist machen sich die Praxen gar keine Gedanken darüber. Das Verhalten ist jedoch gemessen an den Datenschutz- und Schweigepflicht-Regeln höchst bedenklich.

Umorganisation von Abläufen

Wichtig: Wenn von der räumlichen Umsetzung des Datenschutzes gesprochen wird, muss das nicht unbedingt mit größeren Umbaumaßnahmen verbunden sein. Oftmals reichen die Auseinandersetzung mit dem Thema im Team und eine Umorganisation in den einzelnen Abläufen.

Was sind personenbezogene Auskünfte?

Berechtigte Personen

Personenbezogene Auskünfte sind beispielsweise Fragen zu Befunden und zu Behandlungen. Berechtigte Personen, denen man personenbezogene Auskünfte erteilen darf, können mitbehandelnde Ärzte, Angehörige oder Kostenträger sein.

Absolute Diskretion

Diese Informationen sind unbedingt zu schützen. Achten Sie daher auf absolute Diskretion in Ihrer Praxis. Nennen Sie zum Beispiel keine Namen, wenn weitere Patienten in der Nähe sind.

Weitergabe von Auskünften

Befunde und weitere Behandlungsschritte sollten nur im geschlossenen Zimmer weitergegeben werden, oder es muss absolut sichergestellt sein, dass niemand mithört, der nicht dazu befähigt ist.

Verantwortlichkeiten klären

Wichtig: Legen Sie exakt fest, wer in der Praxis welche Auskünfte weitergeben darf und wie die Kommunikation zu erfolgen hat.

Wichtige Maßnahmen beim Umgang mit patientenbezogenen Auskünften:

To-dos

- ✓ Erstellen Sie eine praxisinterne schriftlich dokumentierte Vereinbarung zum Umgang mit patientenbezogenen Auskünften (QM/Arbeitsanweisung: z. B. nach dem Fragenstellen nach Geburtsjahr, Adresse, Versicherungsnummer Angaben nicht laut vorlesen!)

Eine individualisierbare Arbeitsanweisung finden Sie auf beiliegender CD-ROM.

- ✓ Erstellen Sie einen Einarbeitungsplan für neue Mitarbeiter. Dieser Einarbeitungsplan sollte die Datenschutzunterweisung und die Vergabe von Zugangs-, Zugriffsrechten und Passwörtern enthalten.
- ✓ Erstellen Sie eine Checkliste, welche Unterlagen, Dokumente, Zugriffsrechte etc. der Mitarbeiter während des Arbeitsverhältnisses erhält, bzw. was nach Beendigung des Arbeitsverhältnisses an die Praxis zurückgegeben werden muss.

Einfach umzusetzende Praxistipps zur Optimierung des Datenschutzes:

- ✓ Führen Sie im Empfangsbereich eine Diskretionszone ein: