Leitfaden Datenschutz im zahntechnischen Labor

Gesamtinhalt

Wegweiser
Vorwort
Autorenverzeichnis
Glossar

CD-ROM
Benutzerhinweise CD-ROM
Inhalt CD-ROM

Teil 1 Rechtliche Grundlagen
1 Einführung
2 Gesundheitsdaten und Datenschutz
3 Betroffenen-Datenschutz in der DSGVO
4 Das neue Datenschutzrecht im zahntechnischen Labor
5 Häufige Fragen und Antworten zum Datenschutz im zahntechnischen Labor
6 Einzelne datenschutzrechtliche Problembereiche

Teil 2 Technische Voraussetzungen
1 Einführung
2 Datenschutzbeauftragter unter technischen Gesichtspunkten
3 Begriffe der Datenschutz-Grundverordnung
4 Technischer Datenschutz im zahntechnischen Labor
5 Datenschutzrechte
6 Datensicherung
7 Sicherungsstrategien
8 Internet im Laboreinsatz
9 Checklisten und Mustervorlagen

Teil 3 Praktische Umsetzung der EU-Datenschutz-Grundverordnung im zahntechnischen Labor
1 Verantwortungsbereiche und Pflichten beim Datenschutz im zahntechnischen Labor

2 Datenschutzkontrolle
3 Umsetzung des Datenschutzes im zahntechnischen Labor
4 Dokumentation, Archivierung, Vernichtung, Entsorgung und Löschung von Daten
5 Datenschutz als Bestandteil des QMs im zahntechnischen Labor
6 Mitarbeiterunterweisung „Datenschutz & Schweigepflicht“
7 Kundenfragen zur Umsetzung des Datenschutzes im zahntechnischen Labor

4.2 Datenschutzbeauftragter

Wann ist ein Datenschutzbeauftragter erforderlich?

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

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

Voraussetzung f. Erfordernis eines Datenschutzbeauftragten

- Die Einrichtung 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).

Öffentliche Stelle

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

Kerntätigkeit Datenverarbeitung

Ein Datenschutzbeauftragter ist weiter dann zu benennen, wenn die Kerntätigkeit die Durchführung von Datenverarbeitungen betrifft. Auch wenn in dem durchschnittlichen Dentallabor eine Menge von Daten erhoben und verarbeitet werden, ist die Datenverarbeitung jedoch nicht deren Kerntätigkeit. Sie ist vielmehr ein notwendiges „Nebenprodukt" des Betriebes des Labors. Diese Variante des Artikels 37 DSGVO scheidet somit bei dem durchschnittlichen Dentallabor ebenfalls aus.

Kerntätigkeit Verarbeitung von Gesundheitsdaten

Es verbleibt damit das Kriterium des Artikels 37 Absatz 3 DSGVO. Danach ist ein Datenschutzbeauftragter zu benennen, wenn die Kerntätigkeit in der umfangreichen Verarbeitung u. a. von Gesundheitsdaten besteht.

Wann liegt umfangreiche Verarbeitung 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.

Einschätzung für Labor

In Fachkreisen wird die Auffassung vertreten, allein die Tatsache, dass im Dentallabor die besonders sensiblen Gesundheitsdaten verarbeitet werden, führe zu der Verpflichtung gemäß Artikel 37 DSGVO, einen Datenschutzbeauftragten zu bestellen. So vertritt der Sächsische Landesdatenschutzbeauftragte zu der bisherigen Rechtslage nach BDSG-alt folgende Auffassung:

„Wie der Aufsichtsbehörde mitgeteilt worden ist, enthalten die von den Zahnärzten an Dentallabore erteilten Aufträge in der Regel Vor- und Zunamen sowie den Versicherungsstatus des jeweiligen Patienten, mithin also personenbezogene Daten. Wegen der Tatsache, dass es Zweck des erteilten Auftrages ist, durch das Dentallabor nach entsprechenden Vorgaben Zahnersatz anfertigen zu lassen, handelt es sich dabei um Angaben zur Gesundheit des Patienten, mithin um besondere Arten personenbezogener Daten gemäß § 3 Abs. 9 BDSG."

Schlussfolgerung f. Labor

Der Landesdatenschutzbeauftragte zieht daraus den Schluss, dass hieraus die Pflicht zur Bestellung eines Datenschutzbeauftragten folge.

Erwägungsgrund f. Datenschutz-Folgenabschätzung

Hinweise, wie der Begriff auszulegen ist, finden sich aber auch in den Erwägungsgründen der DSGVO. 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".

Erfordernisse im Dentallabor

Aus dieser Betrachtung des Richtliniengebers für die Situation in der Arzt-/Zahnarztpraxis können nach diesseitiger Auffassung auch Schlüsse auf die Erfordernisse im Dentallabor gezogen werden. Geht der Betrieb des Dentallabors vom Umfang der Datenverarbeitung her nicht über den einer Einzelpraxis eines Arztes oder Zahnarztes hinaus, ist es gut vertretbar, auf die Bestellung eines Datenschutzbeauftragten zu verzichten.

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

Weiteres Kriterium f. Bestellung eines DS-Beauftragten

(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 zwanzig 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 Übermittlung, 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."*

Abhängig von Personalgröße

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

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 dem sogenannten Verantwortlichen, also insbesondere der Geschäftsleitung. 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 der Betrieb des Dentallabors einen erheblichen Umfang hat. Das ist insbesondere an der Zahl der beschäftigten Personen zu messen, die regelmäßig Datenverarbeitungsvorgänge im Unternehmen durchführt. Liegt die Zahl über 20 Personen, wobei Betriebsinhaber 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 Bestellung eines Datenschutzbeauftragten finden Sie auf beiliegender CD-ROM

Möglichkeit, Verpflichtung zu umgehen

Eine Möglichkeit, die Pflicht zur Bestellung eines Datenschutzbeauftragten zu umgehen, bleibt gleichwohl. Nämlich dann, wenn durch organisatorische Maßnahmen erreicht wird, dass die personenbezogenen Patientendaten nicht in Klarform übermittelt werden.

Anonymisierter Datenaustausch

Ein Datenaustausch zwischen Dentallabor und Zahnarztpraxis kann auch in anonymisierter Form erfolgen, indem etwa die Zahnarztpraxis die Aufträge nur mit Auftragsnummern versieht und den Patientennamen und seine sonstigen Daten nicht übermittelt. In diesem Fall kann nur die Zahnarztpraxis eine direkte Verbindung zwischen Auftrag und Patient herstellen. Eine Übermittlung personenbezoge-

1.5.1 Durchführung der Mitarbeiterunterweisung im Datenschutz und der Schweigepflicht

Unterweisungspflicht

Mitarbeiter müssen vor Aufnahme ihrer Tätigkeit und zur Sensibilisierung regelmäßig durch den Labor-Verantwortlichen ausführlich unterwiesen werden. Die Unterweisungspflicht ergibt sich aus § 12 Arbeitsschutzgesetz.

Verantwortlichkeit

Der Labor-Verantwortliche ist insbesondere dafür verantwortlich, dass Mitarbeiter von branchenspezifischen Neuerungen wissen, sie kennen und beachten. Die Neuregelungen zum Datenschutz sind im Mai 2018 in Kraft getreten. Mitarbeiter müssen folglich unter anderem über Besonderheiten beim Umgang mit Patientendaten/personenbezogenen Daten aufgeklärt und eingewiesen werden.

Gültigkeitsdauer

Wichtig: Die Einhaltung der Datenschutz- und Schweigepflicht gilt über das Arbeitsverhältnis hinaus. Sollte ein Mitarbeiter das Labor verlassen, ist das Weitererzählen von Internas nicht zulässig.

Unterweisen Sie Ihre Mitarbeiterinnen und Mitarbeiter zu folgenden Aspekten:

Unterweisungsinhalte

- Alle Einzelangaben über persönliche oder sachliche Verhältnisse einer natürlichen Person (Gesundheitsdaten, Kontodaten, Telefonnummern und E-Mail-Adressen etc.) müssen vor Missbrauch geschützt werden. Alle Mitarbeiterinnen und Mitarbeiter sind zur Einhaltung der praxisinternen Schutzmaßnahmen rechtlich verpflichtet. Dies gilt auch nach Beendigung des Arbeitsverhältnisses.
- Zu den besonders schutzwürdigen Gesundheitsdaten eines Patienten gehören nicht nur die Daten wie Befunde, Therapie und Abrechnung. Schon die Information, dass ein Patient in einer bestimmten Zahnarztpraxis behandelt wird oder der Zahnersatz in Ihrem Labor gefertigt wird, ist vom Datenschutz und der Pflicht zur Verschwiegenheit betroffen.
- Jede Mitarbeiterin und jeder Mitarbeiter hat sich bei der Datenerhebung und -verarbeitung immer an die Weisungen des Labor-Verantwortlichen zu halten. Der Mitarbeiter darf nur dann mit

personenbezogenen Daten arbeiten, wenn dies vom Labor-Verantwortlichen erlaubt wurde.

- Personenbezogene Daten müssen vertraulich behandelt werden und dürfen nicht offen liegen gelassen werden. Insbesondere sind Patienten-/Kundendaten, wenn diese nicht mehr benötigt werden, in die dafür vorgesehen Schränke zurückzulegen.
- Mitarbeiterinnen und Mitarbeiter sind nicht berechtigt, ohne Auftrag fremden, mit der Sache nicht befassten Personen Einblick in Post, Patienten-/Kundenunterlagen, Belege und sonstige Unterlagen zu gewähren oder derartige Unterlagen an sich zu nehmen oder sie an Dritte herauszugeben. Dies gilt auch für Abschriften oder Fotokopien dieser Dokumente.
- Mitarbeiterinnen und Mitarbeiter verpflichten sich in ihren Arbeitsverträgen vertraglich dazu, über sämtliche Informationen, die ihnen im Zusammenhang mit den Laborarbeiten oder Behandlung der Patienten bzw. über Kundeninformationen zur Kenntnis gelangen, gegenüber Dritten zu schweigen.
- Das arbeitsvertragliche Schweigegebot beinhaltet auch alle anderen personenbezogenen Daten, die erhoben und verarbeitet werden. Die Verschwiegenheitspflicht besteht insbesondere auch gegenüber eigenen Familienangehörigen sowie gegenüber Familienangehörigen von Patienten und Kunden. Die Mitarbeiterinnen und Mitarbeiter werden auf § 203 Strafgesetzbuch („Verletzung von Privatgeheimnissen“) hingewiesen.
- Mitarbeiterinnen und Mitarbeiter werden auch über die gesetzlichen Bestimmungen zum Zeugnisverweigerungsrecht (§§ 53, 53a Strafprozessordnung) informiert. Wichtig ist hier, dass die Mitarbeiterinnen und Mitarbeiter darauf hingewiesen worden sind, dass sie gegenüber Gerichten und Behörden über Gegebenheiten, die ihnen bei ihrer Tätigkeit bekannt geworden sind, nur nach Genehmigung des Labor-Verantwortlichen Auskünfte erteilen dürfen.
- Neben der Verschwiegenheitspflicht sind die Grundsätze der EU-Datenschutz-Grundverordnung bei der Verarbeitung personenbezogener Daten zu beachten.

Praxisbeispiele zum Risikomanagement

Hinweis: Die folgenden Vorlagen gelten als Beispiele für eine Risikoanalyse und -bewertung, die auf die jeweiligen Laborbegebenheiten angepasst und ggf. ergänzt werden müssen.

Risikoanalyse und -bewertung

Risikobereich:	**Datenschutz und Datensicherheit im Labor**
Risiko-Nr.:	**1**
Art:	**Mitarbeiterqualifikation allgemein**
Risikoanalyse	
Mögliches Risiko/Fehler/ Ausgangslage:	Mitarbeiter können auf Grund fehlender Qualifikation nicht die notwendige Qualität ihrer Arbeit leisten bzw. übersehen rechtliche Vorgaben.
Mögliche Folge des Risikos/ Fehlers:	• Nicht alle im Team sind auf dem gleichen Wissensstand, obwohl in vielen Bereichen notwendig. • Unzufriedenheit Arbeitgeber, Mitarbeiter, Kunde, Patient • Der gute Ruf des Labors kann gefährdet sein. • Fehler bei der Durchführung von Arbeitstätigkeiten • Arbeitsschritte müssen ggf. wiederholt werden. • Fehler können u. U. ein juristisches Nachspiel mit Schadenersatzforderungen haben. • usw.

(Fortsetzung nächste Seite)

* Die Farbangabe bezieht sich auf die farbige Vorlage auf der CD-ROM.

Aktuelle Maßnahmen zur Risikominimierung:	• Mitarbeiter legt Laborleitung (oder umgekehrt) vor, welche Fortbildung (Qualifizierungsmaßnahme) besucht werden könnte.
Risikomatrix: Risikobewertung und Priorisierung	
Eintrittswahrscheinlichkeit und Auswirkungen/ Schadensmaß:	

Auswirkung/ Schadensmaß				
Gering				
Mittel				
Hoch				x
	Eintrittswahrscheinlichkeit	Gering	Mittel	Hoch

Risikobehandlung:
Festlegung neuer Schutzmaßnahmen und Risikobewertung zur Risikominderung, wenn Priorisierung des Risikos/Fehlers im roten* Bereich ist

Neue Maßnahmen:
Stetige Weiterentwicklung steht an oberer Stelle:

- In Mitarbeiter(MA)-Jahresgesprächen werden die Weiterentwicklung besprochen und Schulungen geplant.
- Einmal im Jahr wird ein MA-Beurteilungsgespräch durchgeführt.
- Bei MA-Neueinstellungen wird die angegebene Qualifikation während der Probezeit aktiv überprüft und es findet ein Feedbackgespräch statt.
- Es existiert eine Bestandsliste aller geplanten MA-Schulungen.
- Es existiert eine Bestandliste aller bereits erfolgten Schulungen/Fortbildungen pro MA.
- Schulungen, die alle im Labor betreffen, wie z. B. Datenschutz und Datensicherheit, finden im Labor mit einem externen Schulungsanbieter statt.
- usw.

Erneute Risikobewertung in der Risikomatrix

Eintrittswahrscheinlichkeit und Auswirkungen/ Schadensmaß:

Auswirkung/ Schadensmaß				
Gering				
Mittel				
Hoch		x		
	Eintrittswahrscheinlichkeit	Gering	Mittel	Hoch