

DATENSCHUTZ

DS-GVO-Check: Haben Sie wirklich schon alle Formalitäten in Ihrer Praxis umgesetzt?

von RAin Walburga van Hövell, Bonn, lennmed.de

| Aufgrund von allseits verfügbaren Informationen zur DS-GVO ist davon auszugehen, dass die meisten Zahnarztpraxen das Thema Datenschutz in seiner formalen und praktischen Umsetzung in Angriff genommen haben. Was allerdings nicht bedeutet, dass dies in der Praxis auch einfach (gewesen) wäre. Hier deshalb ein Überblick darüber, welche Probleme sich immer noch in Zahnarztpraxen typischerweise rund um die DS-GVO-Formalitäten ergeben und wie diese gelöst werden können. |

Die Patienteninformation

Gemäß Art. 13 DS-GVO besteht seitens der Datenschutzverantwortlichen eine Informationspflicht bzgl. der Erhebung personenbezogener Daten. Bezogen auf die Patienten wird in einer Zahnarztpraxis dieser Verpflichtung regelmäßig durch eine sogenannte Patienteninformation nachgekommen. So weit, so gut: Aufgrund diverser Vorlagen seitens der Kammern, KZVen oder sonstiger Bezugsquellen dürfte eine solche Patienteninformation für die eigene Praxis kein Problem sein. Allerdings gibt es sehr unterschiedliche Vorgaben dazu, wie diese Informationen an die Patienten kommen sollen. Die jeweils zuständigen Landesdatenschutzbehörden haben dazu verschiedene Vorstellungen.

PRAXISTIPP | Fragen Sie bei Ihrer Landesdatenschutzbehörde nach, wie die Patienteninformation den Empfängern zur Verfügung gestellt werden soll (Reicht z. B. ein Aufsteller im Wartezimmer oder soll die Information den Patienten ausgehändigt werden?). Denn das ist von Bundesland zu Bundesland unterschiedlich!

Die Praxis-Homepage

Dass auf Homepage und Social-Media-Accounts wie Facebook-Fanpages eine Datenschutzerklärung vorzuhalten ist, hat sich mittlerweile herumgesprochen. Datenschutzrechtlich ist aber darüber hinaus ebenso relevant, dass Nutzer auch online in alle Datenverarbeitungen einwilligen müssen, die nicht für die Zurverfügungstellung der Homepage, zur Erfüllung einer gegenseitigen Verpflichtung oder aus einem berechtigten Interesse heraus notwendig sind.

■ Beispiel

Das Nutzertracking durch das Setzen entsprechender Cookies ist nach der Rechtsprechung des Europäischen Gerichtshofes (EuGH) nur noch durch ein sogenanntes Opt-in rechtmäßig (EuGH, Urteil vom 01.10.2019, Az. C-673/17, dejure.org). D. h., dass der Nutzer in personalisierte Werbung oder Datenanalyse ausdrücklich einwilligen muss, indem er praktikablerweise durch einen entsprechend implementierten Cookie-Banner aktiv seine Einwilligung zum Nutzertracking setzt. Die bisher landläufig verwendeten „Opt-outs“ (= in Cookiebannern ist die Einwilligung zum Nutzertracking voreingestellt) reichen hier nicht mehr aus!



Die Praxisinfo muss auch in der richtigen Weise zum Patienten gelangen

Opt-outs sind nicht mehr zulässig!

Bei Kontrollen ist
i. d. R. das Verzeichnis
vorzulegen

Umfang Datenver-
arbeitung ist für den
Einzel-(zahn-)arzt
definiert

Neu: Telemedizin
kann besonders
risikobehaftet sein

DSFA bedeutet:
Es muss auch ein
DSB her

Das Verzeichnis der Verarbeitungstätigkeiten

Jede Zahnarztpraxis muss ein Verzeichnis der Verarbeitungstätigkeiten erstellen, da regelmäßig Gesundheitsdaten und somit besondere Daten gemäß Art. 9 DS-GVO verarbeitet werden. Falls eine Praxis die Umsetzung dieses Projekts noch nicht in Angriff genommen haben sollte – bitte tun Sie es jetzt! Auch wenn es viel Arbeit bedeutet, ist die Erstellung eines Verfahrensverzeichnis vor allem aus den folgenden Gründen hilfreich:

- Zum einem können Sie sich selbst einen Überblick über die eigene Datenverarbeitung und ggf. erforderliche Verbesserungsmaßnahmen verschaffen.
- Zum anderen wird im Falle einer behördlichen Prüfung – aus welchem Grund auch immer – der für die jeweilige Praxis zuständige Datenschutzbeauftragte die Vorlage eines solchen Verzeichnisses fordern.

Die Datenschutzfolgeabschätzung (DSFA)

Nach Art. 35 DS-GVO hat derjenige Verantwortliche eine Datenschutzfolgeabschätzung (DSFA) zu erstellen, der u. a. umfangreich Gesundheitsdaten verarbeitet. Was genau dieses „umfangreich“ bedeutet, ist nur eindeutig für Einzel-(zahn-)ärzte in dem DS-GVO-Erwägungsgrund 91 Satz 5 definiert. Daraus kann aber nicht gefolgert werden, dass

- kein Einzel-(zahn-)arzt mangels umfangreicher Datenverarbeitung regelmäßig eine DSFA vornehmen muss. Denn auch Einzel-(zahn-)ärzte können aufgrund besonders risikobehafteter Verarbeitungen personenbezogener Daten zu einer DSFA verpflichtet sein;
- jede größere Praxis eine DSFA vornehmen muss. Denn auch größere Praxen können eine „nicht umfangreiche“ Datenverarbeitung haben.

PRAXISTIPP | Um zu einem Ergebnis zu kommen, ob nun eine DSFA durchzuführen ist oder nicht, sollte jede Praxis gründlich prüfen, ob bei ihr Datenverarbeitungen durchgeführt werden, die insbesondere beim Einsatz von neuen Technologien ein hohes Risiko für die Rechte und Freiheiten betroffener Personen darstellen. So sieht die Datenschutzkonferenz den Einsatz von Telemedizin-Lösungen zur detaillierten Bearbeitung von Krankheitsdaten als Verarbeitungstätigkeit an, für die eine DSFA gefertigt werden muss.

Insbesondere ist dann mit sich selbst streng ins Gericht zu gehen, falls Patienten in der nahen Vergangenheit (wiederholt) durch der eigenen Praxis zurechenbare Vorfälle zu Schaden gekommen sind.

Der Datenschutzbeauftragte (DSB)

§ 38 Bundesdatenschutzgesetz ist mittlerweile neu geregelt und die Schwelle für die verpflichtende Benennung eines betrieblichen Datenschutzbeauftragten (DSB) ist auf 20 datenverarbeitende Mitarbeiter angehoben worden. Dennoch darf nicht außer Acht gelassen werden, dass auch kleinere Zahnarztpraxen dann einen DSB benennen müssen, sobald sie eine DSFA zu erstellen haben.

Der Auftragsverarbeitungsvertrag (AVV)

Wird die Verarbeitung personenbezogener Daten an einen externen Dienstleister ausgelagert, so ist gemäß Art. 28 DS-GVO mit diesem Dienstleister ein Auftragsverarbeitungsvertrag (AVV) zu erstellen. Bezüglich der allermeisten externen Dienstleistungen (z. B. Fernwartung durch Mitarbeiter des Softwareanbieters) stellt die Erfüllung dieser Datenschutzformalie an sich auch zumeist kein Problem dar.

Die praktische Erfahrung zeigt aber, dass häufig bei Dienstleistern die Einbindung auf die Verschwiegenheitsverpflichtung vergessen wird, die ansonsten kaum Kontakt zu medizinischen Berufsfeldern haben. Deswegen sollte ein entsprechender AVV extra hinsichtlich der Verpflichtung auf das Berufsgeheimnis (Stichwort: § 203 Strafgesetzbuch) überprüft werden.

Weitere Unsicherheiten beim Umgang mit externen Dienstleistern zeigen sich außerdem bei zwei speziellen Berufsgruppen: den selbstständigen Zahntechnikern, denen für die Erledigung eines Auftrags Patientendaten zugeschickt werden, und den Steuerberatern, an die die Lohnbuchhaltung ausgelagert wird. Teilweise wird von deren Seite der Abschluss eines AVV verweigert, weil es nicht nötig sei.

PRAXISTIPP | Ob nun ein AVV nötig ist oder nicht, wird bundesweit durch die jeweils zuständigen Landesdatenschutzbeauftragten unterschiedlich beantwortet. Fragen Sie deshalb in Ihrem konkreten Fall bei dem für Sie zuständigen Landesdatenschutzbeauftragten nach, ob ein AVV mit einem Dentallabor oder dem Steuerberater für Ihre Lohnbuchhaltung abgeschlossen werden muss.

Die Einwilligung des Patienten

Große Unsicherheit besteht nach wie vor bei der Frage, wann und wie eine Einwilligung des Patienten für eine bestimmte Datenverarbeitung eingeholt werden muss.

Dann ist die Patienteneinwilligung einzuholen

Eine Einwilligung seitens der Betroffenen ist immer dann vonnöten, wenn die entsprechende Datenverarbeitung nicht anders gerechtfertigt ist. Keiner Einwilligung bedarf es also z. B. bei einer gesetzlichen Verpflichtung zur Datenübermittlung, bei der Erfüllung des gegenseitigen Behandlungsvertrags, bei einem berechtigten Interesse der Praxis an der Datenverarbeitung gemäß Art. 6 Abs. 1 lit. f) DS-GVO oder wenn ein AVV die Rechtmäßigkeit der Datenverarbeitung abdeckt (siehe dazu auch schon ZP 10/2018, Seite 8).

So ist die Patienteneinwilligung einzuholen

Die Einwilligung muss durch die Betroffenen ausdrücklich und in informierter Weise erfolgen. Weiterhin sind die Betroffenen darüber aufzuklären, dass sie die ihrerseits erteilten Einwilligungen jederzeit mit Wirkung für die Zukunft widerrufen dürfen. Außerdem darf eine gegenseitige Vertragsbeziehung (z. B. der Behandlungsvertrag) nicht davon abhängig gemacht werden,

Verschwiegenheitsverpflichtung nicht vergessen

AVV auch mit Zahntechnikern und dem Steuerberater abschließen?

Wenn die Datenverarbeitung nicht anders gerechtfertigt ist

Ausdrücklich, informiert und mit Widerrufsmöglichkeit

Schriftlichkeit
bei Abrechnungszwecken erforderlich

ob der Patient in eine bestimmte, nicht für den gegenseitigen Behandlungsvertrag notwendige oder vorgeschriebene Datenverarbeitung einwilligt.

PRAXISTIPP | Die Patienteneinwilligung muss nicht schriftlich erfolgen. Eine Ausnahme hiervon besteht nur nach § 10 Abs. 6 GOZ für eine Einwilligung bzgl. der Datenweiterleitung zum Zwecke der Abrechnung. Im Zweifelsfall ist aber eine entsprechende Dokumentation (z. B. in der Patientenakte) immer unter dem Gesichtspunkt der Beweisbarkeit hilfreich. Vergessen Sie außerdem nicht, dass Sie sich bzgl. der Einwilligung zur Datenweiterleitung von Gesundheitsdaten auch von der Schweigepflicht entbinden lassen müssen.

Daten sind zu löschen, wenn sie nicht aufbewahrt werden dürfen

Das Löschen von Patientendaten

Eine der schwierigsten datenschutzrechtlichen Vorgaben scheint in der Praxis das Löschen von Daten zu sein. Zum einem, weil die Behandler dies teilweise gar nicht wollen. Und zum anderen, weil sie es teilweise rein technisch gar nicht umsetzen können. Doch es gilt:

Personenbezogene Daten müssen immer nach den Grundsätzen des Art. 5 DSGVO behandelt werden. Dazu gehören u. a. die Rechtmäßigkeit der Datenverarbeitung, deren Zweckbindung, Datenminimierung und Speicherbegrenzung, nicht aber ausdrücklich auch das Löschen. Trotzdem ist daraus zu schließen, dass die Daten gelöscht werden müssen, wenn die Rechtmäßigkeit einer Datenspeicherung wegfällt (z. B. weil die Aufbewahrungsfrist der Behandlungsdokumentation abgelaufen ist) oder wenn für die weitere Archivierung eine gesetzliche Rechtsgrundlage fehlt. Wenn der Betroffene nicht in eine unbegrenzte Speicherung einwilligt, kann gar nicht anders mit den Daten verfahren werden, als sie zu löschen. Auch ein berechtigtes Interesse des Behandlers würde dann nur eine weitere Datenspeicherung im Einzelfall rechtfertigen können, nicht aber eine gesamte Behandlungsdokumentation.

MERKE | Logische Konsequenz von allem scheint nur das Löschen von Daten zu sein, wenn diese nicht mehr aufbewahrt werden dürfen. In naher Zukunft wird dieses Thema wohl durch die Immobiliengesellschaft Deutsche Wohnen gerichtlich ausgefochten werden. Denn sie erhielt ein Rekordbußgeld von 14,5 Mio. Euro für ihren „Datenfriedhof“.

Bei Fragen
Fachmann oder
Datenschutzbehörde
kontaktieren

FAZIT | Allein schon wegen rechtlicher Unsicherheiten wird eine 100 Prozent richtige Umsetzung von DS-GVO-Vorgaben nicht möglich sein. Allerdings stellt dies keinen Blankoscheck dafür aus, die Hände in den Schoß zu legen. Bei Fragen kann bei den zuständigen Datenschutzbehörden Rat angefragt oder anderweitig entsprechende professionelle Hilfe eingeholt werden. Jede Zahnarztpraxis muss sich nach wie vor mit dem Thema Datenschutz auseinandersetzen und deswegen auch zwangsläufig die dort geforderten Formalien in Angriff nehmen. Die Datenschutzformalien sollen dazu dienen – auch wenn dies auf den ersten und vielleicht auch zweiten oder dritten Blick anders erscheinen mag –, dass letztlich rechtmäßig mit fremden personenbezogenen Daten umgegangen wird.