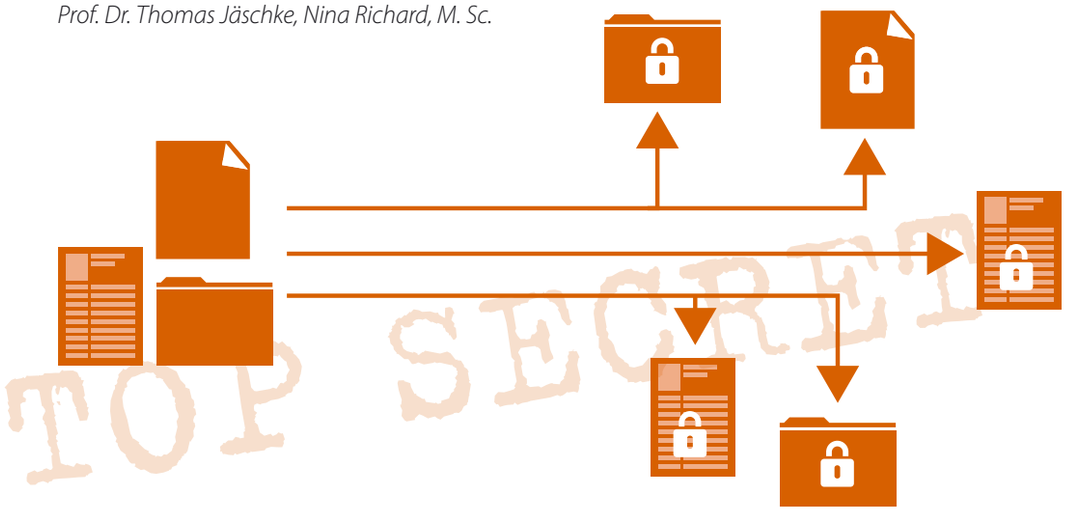
Dentallabore – Datenschutzrechtlich unbedenklich?

So bewegen Sie Ihre Patientendaten sicher von A nach B

Prof. Dr. Thomas Jäschke, Nina Richard, M. Sc.



Aus der Datenschutzperspektive kann die Zusammenarbeit mit Dentallaboren „problematisch“ sein, wenn diese rechtlich gesehen nicht der Zahnarztpraxis angehören, denn in diesem Fall werden hochsensible Daten weitergegeben. Dies ist nur unter bestimmten Rahmenbedingungen erlaubt. Werden diese nicht beachtet, können Zahnärzte sich strafbar machen.

Grundlegende Datenschutzregelungen personenbezogener Daten

Die gesetzliche Definition von personenbezogenen Daten ist im Bundesdatenschutzgesetz (§ 9 BDSG) definiert. Demnach sind Daten, die Auskunft über sachliche oder persönliche Verhältnisse einer Person geben, als personenbezogene Daten zu bezeichnen. Hierzu zählen beispielsweise die Adresse oder Telefonnummer eines Patienten. Nicht immer ist allerdings klar, bei welchen Daten es sich um personenbezogene Daten handelt. So beschäftigte die Frage, inwieweit eine IP-Adresse zu den personenbezogenen Daten gezählt werden kann, bereits mehrfach die Gerichte.

Zahnärztliche Praxen arbeiten allerdings mit einer besonderen Art von personenbezogenen Daten, nämlich mit Gesundheitsdaten. Diese sind besonders schützenswert und dürfen nicht ohne Weiteres weitergegeben und verarbeitet werden. Es herrscht ein Verarbeitungsverbot mit Erlaubnisvorbehalt.

Das heißt, zahnärztliche Praxen dürfen diese Daten ausschließlich für die medizinische Behandlung innerhalb der eigenen Praxis nutzen oder wenn ein Gesetz die Verarbeitung erlaubt (z.B. bei der Abrechnung mit Krankenkassen). Sobald ein externer Dienstleister in die zahnärztliche Behandlung einbezogen wird, der diese Daten weiterverarbeitet (z. B. privatzahnärztliche Abrechnungsstellen oder Dentallabore), muss geprüft werden, wie die genaue gesetzliche Ausgestaltung der Dienstleistung ist. Es kann sich in solchen Fällen entweder um eine sogenannte Funktionsübertragung oder aber eine Auftragsdatenverarbeitung handeln.

Nachfolgend soll der konkrete Fall „Dentallabore“ näher betrachtet werden.
Dentallabore können in verschiedenen Ausprägungen existieren, vor deren Zusammenstellung sich die rechtliche Grundlage zur Verarbeitung der Daten entsprechend ändert und somit auch die datenschutzkonforme Gestaltung der Leistung.

1. Das Dentallabor ist der eigenen Zahnarztpraxis zugeordnet
Vorausgesetzt zahntechnische Leistungen werden im praxiseigenen Labor erbracht, gilt dieses als Hilfsbetrieb unter zahnärztlicher Leitung. Gemäß der MBO-ZÄ muss das praxiseigene Labor nicht zwingend in den Räumlichkeiten der Zahnarztpraxis betrieben werden (vgl. § 11 MBO-ZÄ). Der Zahnarzt muss die fachliche Anleitung sowie Beaufsichtigung seiner Mitarbeiter sicherstellen. Demnach gilt es, die Mitarbeiter auf den Datenschutz zu verpflichten, regelmäßig im Umgang mit personenbezogenen Daten zu schulen und genau wie in der Praxis auch, die technischen und organisatorischen Maßnahmen (z. B. Diskretionsbereich einrichten, automatische Bildschirmsperrung bei den Praxisrechnern, o. ä.) einzuhalten.

Hinweis:
Sind mehr als neun Mitarbeiter mit der Verarbeitung von Daten betraut, ist ein Datenschutzbeauftragter zu bestellen.

2. Das Dentallabor ist externer Dienstleister
Externe Dentallabore sind Betriebe, deren Beziehung mit der zahnärztlichen Praxis innerhalb eines Werkvertrages bestimmt wird. Das Dentallabor ist somit gewerblicher Partner des Zahnarztes und tritt gegenüber dem Patienten nicht in Erscheinung. Der Zahnarzt schließt in diesem Rahmen einen Werkvertrag mit dem Dentallabor sowie einen Behandlungsvertrag mit dem Patienten ab. Je nach Konstellation, wenn personenbezogene Daten übertragen werden, muss zusätzlich noch ein Vertrag zur Auftragsdatenverarbeitung zwischen dem Zahnarzt und dem Dentallabor geschlossen werden.

Die Auftragsdatenverarbeitung ist an die engen gesetzlichen Voraussetzungen des § 11 BDSG gekoppelt und wird als weisungsgebundene Tätigkeit des Dienstleisters verstanden. Bei der Auftragsdatenverarbeitung liegt die datenschutzrechtliche Verantwortung für die Verarbeitung und Nutzung der Gesundheitsdaten beim Zahnarzt. Er gilt als verantwortliche Stelle („Herr der Daten“) und ist für die Gewährleistung der datenschutzkonformen Umsetzung der technischen und organisatorischen Maßnahmen beim Dienstleister verantwortlich. Dem Dienstleister wird nur die tatsächliche Verarbeitung nach Weisung und unter Verantwortung des Auftraggebers, gewissermaßen als sein verlängerter Arm, übertragen. Bei der Datenverarbeitung im Auftrag wird damit lediglich eine Teilfunktion der eigentlichen Aufgabe ausgelagert, ohne dass der Dienstleister einen eigenen Handlungs- oder Entscheidungsspielraum hat. Werden dagegen die der Verarbeitung zugrunde liegenden Aufgaben oder Geschäftszwecke ganz oder teilweise abgegeben, erbringt der Dienstleister über die technische Durchführung hinaus Leistungen mithilfe der überlassenen Daten oder bestehen Handlungs- und Entscheidungsspielräume bei der Erledigung der Aufgabe, liegt eine Funktionsübertragung vor. In diesem Fall wird der Dienstleister zur Daten verarbeitenden und somit verantwortlichen Stelle und hat eigenständig für die datenschutzrechtlichen Vorgaben durch die Umsetzung der erforderlichen technischen und organisatorischen Maßnahmen zu sorgen.

Die Funktionsübertragung findet keine ausdrückliche gesetzliche Grundlage. Bedingt durch die Übertragung der datenschutzrechtlichen Verantwortung handelt es sich hierbei um eine Datenübermittlung (§ 3 Abs. 4 Nr. 3 BDSG), welche nur zulässig ist, wenn entweder eine gesetzliche Grundlage diese legitimiert oder eine Einwilligung des Betroffenen vorliegt.

Zusammengefasst werden folgende Punkte als Erkennungsmerkmale einer Auftragsdatenverarbeitung definiert:

- fehlende Entscheidungsbefugnis des Dienstleisters
- Weisungsgebundenheit des Dienstleisters bezüglich dessen, was mit den Daten geschieht
- Umgang nur mit personenbezogenen Daten, die der Auftraggeber zur Verfügung stellt, es sei denn, der Auftrag ist auch auf die Erhebung von Daten gerichtet
- Ausschluss der Verarbeitung oder Nutzung der Daten zu eigenen Zwecken des Dienstleisters
- keine (vertragliche) Beziehung des Dienstleisters zum Betroffenen.

Zusammengefasst werden folgende Punkte als Erkennungsmerkmale einer Funktionsübertragung definiert:

- Weisungsfreiheit des Dienstleisters bezüglich dessen, was mit den Daten geschieht
- Überlassung von Nutzungsrechten an den Daten
- eigenverantwortliche Sicherstellung von Zulässigkeit und Richtigkeit der Daten durch den Dienstleister, einschließlich des Sicherstellens der Rechte von Betroffenen (Benachrichtigungspflicht, Auskunftsanspruch)
- Handeln des Dienstleisters (gegenüber dem Betroffenen) in eigenem Namen
- Entscheidungsbefugnis des Dienstleisters in der Sache.

Denken Sie an die Schweigepflicht

Im Gesundheitswesen werden die datenschutzrechtlichen Vorschriften durch die berufliche Schweigepflicht der Zahnärzte ergänzt. Man spricht in diesem Zusammenhang von der „Zwei-Schranken-Theorie". Diese besagt, dass für Patientendaten sowohl die Anforderungen des Datenschutzes als auch die der Schweigepflicht erfüllt sein müssen. Dies hat direkte Auswirkungen auf das Konstrukt der Auftragsdatenverarbeitung. In Industrieunternehmen stellt es mittels des Konzeptes der Auftragsdatenverarbeitung keine Herausforderung dar, die Kundendatenbank auf externe Server eines Anbieters auszulagern. Bei der Übertragung dieses Szenarios auf eine zahnärztliche Praxis werden aus klassischen Kunden Patienten, deren Daten dem Zahnarzt während seiner Tätigkeit anvertraut worden sind und somit der zahnärztlichen Schweigepflicht unterliegen. Ein Vertrag zur Auftragsdatenverarbeitung kann nur die datenschutzrechtliche Schranke „heben", die der zahnärztlichen Schweigepflicht bleibt jedoch „geschlossen". Hierdurch ist die Verarbeitung durch einen Dienstleister nicht zulässig. Dies liegt darin begründet, dass dem Zahnarzt offenbarte Daten nur durch ihn und seine Erfüllungsgehilfen zur Kenntnis genommen werden dürfen.

Dem Kreis der Erfüllungsgehilfen werden insbesondere keine Personen hinzugerechnet, die ihre Tätigkeit in einer anderen Gesellschaft ausüben. Dabei ist es unerheblich, ob die Gesellschaften sich in einer Holding- oder Konzernstruktur befinden. Dies führt unter anderem dazu, dass beispielsweise die Auslagerung der IT, aber auch anderer Abteilungen, die für ihre Tätigkeit Zugriff auf patientenbezogene Daten haben, in eine Servicegesellschaft aus Sicht der ärztlichen Schweigepflicht eigentlich nicht zulässig ist. Die zuständigen Aufsichtsbehörden sind sich dieser Problematik bewusst und bei Prüfungen dieses Sachverhalts in der Regel wohlwollend eingestellt.

Was Sie letztendlich beachten müssen

Die Auftragsdatenverarbeitung stellt oftmals das einzige Mittel dar, rechtlich, praktikabel und ohne gesonderte Einwilligungserklärung des Patienten eine Verarbeitung personenbezogener Daten durch Dienstleister zu realisieren. Weiter gilt es, im Gesundheitswesen auch immer die zahnärztliche Schweigepflicht zu berücksichtigen. Dies hat zur Folge, dass sensible Daten durch geeignete Maßnahmen vor unerlaubter Offenbarung geschützt werden müssen, wenn diese an externe Dienstleister abgegeben werden.

3. Das Dentallabor ist mehreren Praxen zugehörig

Beteiligt sich der Zahnarzt an einem gemeinschaftlich betriebenen Dentallabor, bei dem Raum, Geräte und Mitarbeiterkosten geteilt werden, darf es allerdings datenschutzrechtlich nicht zu einer Vermischung des Patientenstammes kommen. Technisch gilt es, dies durch eine entsprechende Mandantentrennung vorzunehmen. Organisatorisch sollten beispielsweise Patientenakten in unterschiedlichen Schränken gelagert oder durch unterschiedlich farbige Akten gekennzeichnet werden. Zudem hat der Zahnarzt jeden Mitarbeiter innerhalb der Personalverträge auf die Schweigepflicht zu verpflichten.

Pseudonymisierung von Daten

Die Pseudonymisierung von Daten befreit den Zahnarzt zwar nicht vor Pflicht der Auftragsdatenverarbeitung, jedoch kann eine gute Pseudonymisierung dem Verstoß gegen die ärztliche Schweigepflicht entgegen wirken. Hier werden die personenidentifizierbaren Merkmale (z.B. Vor- und Nachname, Adresse, o.ä.) mit einer bestimmten Zuordnungsregel durch Pseudonyme ersetzt. Diese kann auch in Form einer Kodierung möglich sein. Durch die Pseudonymisierung bleibt die Interpretierbarkeit der Ergebnisse erhalten, ohne dass die Person von Unbefugten entsprechend identifiziert werden kann.

Quellen:

BZÄK/KZBV - Zahnmedizin und Zahntechnik – Rechtsgrundlagen und Hinweise für die Zahnarztpraxis (2015) S. 4-12.

BDSG, Bundesdatenschutzgesetz, URL: https://www.gesetze-im-internet.de

Prof. Dr. Thomas Jäschke
Vorstand ISDSG

- *1992: Studium der Informatik, Gründung des Unternehmens C. & C. Jäschke*
- *1996 – 2008: Gründer und Geschäftsführer der Internet Service Professional GmbH (jetzt CompuGroup AG), Entwicklung des jesaja.net-Zuweiserportals (ISPRO GmbH), Platzierung von CORDOBA für Arztnetze am Markt*
- *2008 – heute: Gründung und Leitung des Institutes für Sicherheit und Datenschutz im Gesundheitswesen (ISDSG), Datenschutzbeauftragter für Unternehmen, Umsetzung von Datenschutz- und Sicherheitskonzepten*
- *seit 2014: Vorstand der DATATREE AG*

Die Schwerpunkte seiner Professur an der FOM Hochschule für Ökonomie & Management sind IT-Security, Mobile Computing und Informationsmanagement. Seit Januar 2015 betreut Prof. Jäschke als wissenschaftlicher Leiter den Hochschulbereich IT Management, der sowohl einen Bachelor- wie Masterstudiengang beinhaltet.

Nina Richard, M. Sc.

Nina Richard, M. Sc. ist Leiterin Marketing und Kommunikation bei DATATREE AG/ISDSG, Institut für Sicherheit und Datenschutz im Gesundheitswesen. Zudem betreut Sie die Fort- und Weiterbildungsangebote wie den zertifizierten Datenschutzbeauftragten (IOM) und die Angebote der DATATREE-Akademie.