Der Hamburgische Beauftragte für
Datenschutz und Informationsfreiheit

# Datenschutz in Arzt- und Zahnarztpraxen

[Stand: Februar 2019]

*Die hohe Zahl der Beratungsanfragen von Ärzten und Patienten zeigt erhebliche Unsicherheiten bei der Umsetzung der DSGVO im Hinblick auf die Komplexität der maßgeblichen Regelungen. Wir haben die fünf meistgestellten Fragen zum Datenschutz in Arzt- und Zahnarztpraxen ermittelt und in dieser Handreichung beantwortet.*

Gesundheitsdaten[1] zählen zu den auch im neuen Datenschutzrecht gemäß Art. 9 Datenschutz-Grundverordnung (DSGVO) besonders geschützten Kategorien personenbezogener Daten. Ihre Verarbeitung ist verboten – es sei denn, dass eine oder mehrere der in Art. 9 Abs. 2 DSGVO normierten Ausnahmen greifen. Die für die Datenverarbeitung in Arzt- und Zahnarztpraxen wichtigsten Ausnahmen regelt Art. 9 Abs. 2 lit. h DSGVO. Die Herausforderung der Vorschrift liegt in ihrem komplexen Zusammenspiel mit Regelungen des nationalen Zivilrechts, des ärztlichen Berufsrechts und des Sozialrechts sowie der Bezugnahme auf die personellen Einschränkungen in Art. 9 Abs. 3 DSGVO. Herausfordernd gestaltet sich auch die Klärung, unter welchen Voraussetzungen welche Organisations- und Verfahrenspflichten (Benennung eines Datenschutzbeauftragten, Datenschutz-Folgeabschätzung, Meldung nach Art. 33 DSGVO u.a.) von einer Arztpraxis zu beachten sind.

Die komplizierte Rechtslage auf der einen und verschiedentlich geschürte Ängste vor Abmahnungen und Bußgeldern auf der anderen Seite sind ursächlich dafür, dass sich das Beratungsaufkommen zum Thema „Datenschutz in Arztpraxen“ in unserer Dienststelle im vergangenen

[1] Personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen (Art. 4 Nr. 15 DSGVO).

www.hamburg.datenschutz.de
E-Mail: mailbox@datenschutz.hamburg.de
Ludwig-Erhard-Str. 22 - D-20459 Hamburg - Tel.: 040 - 4 28 54 - 40 40 - Fax: 040 - 4 28 54 – 40 00
Vertrauliche Informationen sollten auf elektronischem Weg nur verschlüsselt an uns übermittelt werden.
Unser öffentlicher PGP-Schlüssel ist im Internet verfügbar (Fingerprint: 0932 579B 33C1 8C21 6C9D E77D 08DD BAE4 3377 5707).

Jahr um ein Vielfaches erhöht hat. Die folgenden fünf Fragen, die wir hier mit Antworten vorstellen, belegen die Spitzenplätze der von uns ermittelten FAQs:

**1. Wie sind die Informationspflichten nach Art. 13 und 14 DSGVO in der Arztpraxis umzusetzen?**

Jeder Arzt, jede Berufsausübungsgemeinschaft (BAG) und jedes Medizinische Versorgungszentrum (MVZ) hat als Verantwortlicher den Patienten die in Art. 13 und 14 DSGVO genannten Informationen über die Verarbeitung ihrer Daten bereitzustellen.

In erster Linie sollen die Patienten über die Tatsache der Datenverarbeitung, die Person des Verantwortlichen und ggf. des Datenschutzbeauftragten, die Zwecke und Rechtsgrundlagen der Verarbeitung sowie die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten informiert werden (Art. 13 Abs. 1 DSGVO). Daneben ist in Art. 13 Abs. 2 DSGVO die Mitteilung weiterer Informationen vorgesehen, insbesondere der Speicherdauer (oder falls nicht möglich diesbezüglicher Kriterien) und des Bestehens der Betroffenenrechte nach Artt. 15 ff. DSGVO sowie des Beschwerderechts bei einer Aufsichtsbehörde (in Hamburg: beim HmbBfDI). Werden die Daten nicht direkt bei den Betroffenen, sondern bei Dritten erhoben, muss zusätzlich mitgeteilt werden, um welche Kategorien von Daten es sich handelt und aus welchen Quellen diese Daten stammen.

Die Information der Patienten, die in der Praxis behandelt werden, kann durch gut sicht- und lesbare Aushänge an verschiedenen, besonders frequentierten Orten der Praxis erfolgen (Rezeption, Wartezimmer o. ä.). Zusätzlich sollten die Informationen als Handzettel ausgelegt und bei der Erstaufnahme eines Patienten auf die Informationen und die Mitnahmemöglichkeit hingewiesen werden. Es genügt, wenn auf dem Handzettel nur die wichtigsten Informationen zusammengefasst und für die weiteren Einzelheiten auf den Aushang in der Praxis und/oder die Veröffentlichung auf der Praxiswebsite verwiesen wird. Bei Veröffentlichung auf der Praxiswebsite ist darauf zu achten, dass sich die Informationen zur Datenverarbeitung in der Arztpraxis deutlich von der Datenschutzerklärung zur Website unterscheiden.

Werden Patienten ausschließlich außerhalb der Praxis behandelt (bspw. Behandlung im Pflegeheim oder im Rahmen von Bereitschafts- und Notdiensten), muss deren Information am Behandlungsort erfolgen, etwa durch Aushändigung eines Handzettels.

Patienten müssen die Datenschutzinformation nicht unterschreiben. Allerdings sollte auf eine belastbare Art und Weise dokumentiert werden, dass eine Information erfolgt ist (s. dazu auch unten unter 3.).

**2. Wann muss im Rahmen der ärztlichen Behandlung von Patienten eine Einwilligungserklärung eingeholt werden?**

Die Erhebung, Speicherung und Nutzung von Gesundheitsdaten durch einen behandelnden Arzt, eine BAG oder ein MVZ ist im Rahmen des Behandlungsvertrages und dem zur Behandlung erforderlichen Umfang ohne Einwilligungserklärung der Patientin/des Patienten von Gesetzes wegen zulässig (vgl. Art. 9 Abs. 2 lit. h letzte Alternative DSGVO). Demnach dürfen insbesondere Name, Kontaktdaten und Versicherungsnummer des Patienten, die Anamnese- und Behandlungsdokumentation, Arztbriefe und Laborberichte in der Arztpraxis auch ohne Einwilligung verarbeitet werden.

Auch die Übermittlung dieser Patientendaten zwischen mehrere Ärztinnen und/oder Ärzten, die gleichzeitig oder nacheinander dieselbe Patientin/denselben Patienten untersuchen oder behandeln, kann – analog der Regelungen zur Schweigepflicht – ohne Einwilligung erfolgen, sofern Anhaltspunkte dafür vorliegen, dass das Einverständnis der Patientin/des Patienten anzunehmen ist und § 73 Abs. 1b SGB V nicht entgegensteht. Andernfalls ist die Übermittlung zwischen den behandelnden Ärzten nur auf der Grundlage einer Einwilligung zulässig.

*Beratungsschwerpunkt Laborbeauftragung*

Vorstehendes gilt auch für die Datenübermittlung zwischen behandelndem Arzt und beauftragtem Laborarzt. Nach unserer Auffassung handelt es sich bei der Erteilung von Laboraufträgen an einen Laborarzt nicht um ein Auftragsverarbeitungsverhältnis zwischen behandelndem Arzt und Laborarzt. Dem steht zum einen die besondere Fachkunde des Laborarztes entgegen, die bei einer streng weisungsgebundenen laborärztlichen Tätigkeit nicht zum Tragen kommen könnte. Zum anderen erfolgt die Beauftragung des Laborarztes aber auch nicht im eigenen Namen des behandelnden Arztes, sondern namens und mit stillschweigender Vollmacht des Patienten. Der behandelnde Arzt übermittelt die Patientendaten daher nicht als Verantwortlicher, sondern – sofern ein Einverständnis der Patientin oder des Patienten mit der Laboruntersuchung anzunehmen ist – in seiner Funktion als Vertreter des Patienten. Es bedarf daher keines Auftragsverarbeitungsvertrages nach Art. 28 DSGVO. Allerdings sind die Patienten entsprechend Art. 13 Abs. 1 lit. e DSGVO darüber zu informieren, an welchen Laborarzt Patientendaten übermittelt werden.

Dentallabore sind demgegenüber im Verhältnis zu dem beauftragenden Zahnarzt als Auftragsverarbeiter einzustufen, weshalb zwischen beiden ein Auftragsverarbeitungsvertrag abgeschlossen werden muss.

*Beratungsschwerpunkt Praxisgemeinschaft*

Da es sich bei den Ärzten einer Praxisgemeinschaft nicht per se um mitbehandelnde Ärzte handelt, bedarf die Datenübermittlung zu Vertretungszwecken innerhalb einer Praxisgemeinschaft der Einwilligung des Patienten. Die zwischen den Ärzten bzw. den Praxen der Praxisgemeinschaft vereinbarten Vertretungsregelungen rechtfertigen für sich genommen ebenso wenig den Zugriff auf die Daten der durch den jeweils anderen Praxispartner behandelten Patienten, wie die üblicherweise gemeinsame Nutzung eines Praxisinformationssystems. Der Zugriff auf die Patientendaten der anderen Praxen der Praxisgemeinschaft muss vielmehr durch technisch-organisatorische Maßnahmen, wie insbesondere eine logische oder physikalische Trennung der Datenbestände, verhindert werden.

*Beratungsschwerpunkt Abrechnung*

Die Abrechnung über die Kassenärztliche Vereinigung Hamburg (KVH) bzw. über die Kassenzahnärztliche Vereinigung Hamburg (KZV HH) ist gesetzlich im SGB V geregelt und bedarf daher keiner Einwilligung.

Anders hingegen die Einschaltung einer Abrechnungsstelle für privatärztliche Leistungen. Sowohl die Datenübermittlung an die Abrechnungsstelle als auch die dortige Verarbeitung der übermittelten Daten setzt – sofern die Abrechnungsstelle nicht lediglich als Auftragsverarbeiter tätig wird (dazu unten) – eine wirksame Einwilligungserklärung der Patientin/des Patienten voraus. Dasselbe gilt für eine etwaige Bonitätsüberprüfung von Privatpatienten über Auskunfteien wie die Schufa, für die zusätzlich eine Schweigepflichtentbindungserklärung eingeholt werden muss. Die Wirksamkeit der Einwilligung hängt dabei neben der Informiertheit auch von der Freiwilligkeit der Erteilung ab, die bei drohender Behandlungsablehnung für den Fall der Einwilligungsversagung ebenso wie bei Berechnung eines zusätzlichen Entgelts für eine praxisintern erstellte Abrechnung regelmäßig zu verneinen sein dürfte.

Erfolgt keine Abtretung der Honorarforderung an die Abrechnungsstelle, sondern verbleibt diese beim Arzt selbst, kann die Abrechnung als Auftragsverarbeitung ausgestaltet werden. Dazu bedarf es datenschutzrechtlich eines Vertrags zur Auftragsverarbeitung (Art. 28 DSGVO). Wird die Forderung hingegen an die Abrechnungsstelle abgetreten, wird die Abrechnungsstelle in keinem Fall als Auftragsverarbeiter tätig, sondern ist selbst Verantwortlicher.

*Beratungsschwerpunkt Service-Leistungen*

Sofern eine Arztpraxis zusätzliche Dienste wie z.B. einen Newsletter oder Recall-Service anbieten will, ist die diesbezügliche Verarbeitung von Patientendaten aufgrund des nicht durch den Behandlungsvertrag gedeckten Zwecks nur mit Einwilligung der Patientin/des Patienten zulässig.

**3. Darf die ärztliche Behandlung verweigert werden, wenn der Patient den Erhalt der Datenschutzinformationen nicht quittiert und/oder nicht in die Verarbeitung personenbezogener Daten einwilligt?**

Nein, eine Behandlungsverweigerung wegen Nichtquittierung der Datenschutzinformationen oder Ablehnung einer Einwilligungserklärung kann weder auf die Informationspflicht nach Art. 13 DSGVO und die Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO, noch auf das Verarbeitungsverbot des Art. 9 Abs.1 DSGVO gestützt werden.

Die Informationspflicht nach Art. 13 DSGVO dient dazu, den Patienten Gelegenheit zur einfachen und direkten Kenntnisnahme der Informationen zu geben. Eine Verpflichtung es Betroffenen zur Kenntnisnahme ist Art. 13 DSGVO demgegenüber nicht zu entnehmen. Der Arzt kann den Nachweis einer ordnungsgemäßen Informationserteilung gegenüber der Aufsichtsbehörde auch dadurch führen, dass er den üblichen Verfahrensablauf zur Umsetzung der Informationspflichten dokumentiert und ggf. die Aushändigung von Unterlagen vermerkt (vgl. dazu den Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder [DSK] vom 5. September 2018).

Weiter sind die gesetzlichen Voraussetzungen für die zur Behandlung erforderliche Datenverarbeitung auch ohne Einwilligung erfüllt (s. dazu Frage 1), sodass eine nicht erteilte Einwilligung für sich genommen einer Behandlung nicht entgegensteht.

**4. Ist die Übermittlung von Patientendaten (Befunden, Arztbriefen u. ä.) per E-Mail oder per Fax zulässig?**

Angesichts der Sicherheitsanforderungen an die Verarbeitung von Gesundheitsdaten (vgl. dazu Art. 32 DSGVO und § 22 Abs. 2 BDSG) gilt für diese Daten sowohl bei der elektronischen Speicherung als auch bei der elektronischen Übermittlung grundsätzlich eine Verschlüsselungspflicht. Das heißt, dass ein Versand von Patientendaten mittels einfacher (allenfalls transport-, nicht aber Ende-zu-Ende-verschlüsselter) E-Mail regelmäßig keinen zulässigen Übermittlungsweg darstellt. Das gilt auch dann, wenn der Patient sich ausdrücklich mit dem Versand per einfacher E-Mail einverstanden erklärt hat, da die Verpflichtung zur Gewährleistung eines angemessenen Schutzniveaus nicht durch eine Vereinbarung zwischen Praxis und Patient abbedungen werden kann. Eine Übermittlung von Gesundheitsdaten wie Diagnosen, Krankheitsverläufen, Arzt- und Befundberichten, radiologischen Bildern oder Symptombeschreibungen per einfacher E-Mail ist daher nur dann vertretbar, wenn die „Umstände der Verarbeitung“ (vgl. Art. 32 DSGVO) den Verschlüsselungsverzicht rechtfertigen. Dies kann zum Beispiel bei medizinischen Notfällen aufgrund der

Dringlichkeit oder bei wechselndem Auslandsaufenthalt des Patienten mangels Erreichbarkeitsalternativen der Fall sein. Demgegenüber dürfen einfache Terminanfragen und -absagen, die neben dem Patientennamen und dem Kalenderdatum des angefragten/abgesagten Termins keine Gesundheitsdaten enthalten, aufgrund ihrer vergleichsweise geringen Sensibilität generell unverschlüsselt übermittelt werden.

Da im Regelfall davon auszugegangen werden muss, dass bereits eine Umstellung des Telefonnetzes auf eine IP-basierte Datenübermittlung (All-IP) erfolgt ist, bestehen bei einer Faxübermittlung die gleichen Sicherheitsbedenken wie bei dem Versand von Gesundheitsdaten mittels einfacher E-Mail. Denn der von den Diensteanbietern zum Schutz der ausgetauschten personenbezogenen Daten zu gewährleistende Stand der Technik kann allenfalls eine hinreichende Sicherheit vom Server des Absenders zum Server des Empfängers bedingen, nicht aber vom jeweiligen Faxgerät zum Server. Eine IP-basierte Fax-Übermittlung darf daher ebenfalls nur ausnahmsweise aufgrund der im Rahmen der Bestimmung des Schutzniveaus zu berücksichtigenden Umstände der Verarbeitung erfolgen, namentlich dann, wenn ein Postversand der Gesundheitsdaten in medizinischer Hinsicht zu lange dauern würde. Außer in Notfallsituationen kann ein solcher Fall beispielsweise auch dann vorliegen, wenn durch eine Postübermittlung die notwendige Weiterbehandlung im jeweiligen Einzelfall nachweislich verzögert würde, etwa weil der umgehend notwendige Termin beim Nachbehandler schon für den Folgetag terminiert ist. Wird demgegenüber sorgfaltswidrig ein umgehender Postversand versäumt und ist nur deshalb die rechtzeitige postalische Übermittlung nicht mehr möglich, kann dies grundsätzlich keinen Faxversand rechtfertigen.

Bejaht man unter diesen Voraussetzungen die Möglichkeit des Faxversandes, ist in organisatorischer Hinsicht sicherzustellen, dass im Rahmen der Abgangskontrolle Adressat und Faxnummer (insbesondere die Aktualität gespeicherter Nummern) kontrolliert werden und die Übersendung beim Adressaten telefonisch angekündigt wird, so dass auch dort nur Berechtigte von den Daten Kenntnis nehmen können. Eine telefonische Ankündigung ist dann nicht erforderlich, wenn sich der Absender beim Empfänger vergewissert hat, dass aufgrund des Standorts des Empfängerfaxgeräts kein Unbefugter Kenntnis von dem Fax nehmen kann. In technischer Hinsicht sind außerdem die Hinweise des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur Realisierung von Schutzkonzepten bei IP-Telefonie sowie die Empfehlungen der Bundesnetzagentur für einen möglichst fehlerfreien Betrieb analoger Faxgeräte bei IP-basierter Übertragung (vgl. https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Technik/ATRT/IPMigration/IPMigration-node.html) zu beachten. Sofern Dokumente zum Faxen über W-LAN an einen Multifunktionsdrucker gesendet werden, muss das drahtlose lokale Netzwerk erhöhten Sicherheitsanforderungen genügen.

**5. Wann muss eine Arztpraxis einen Datenschutzbeauftragten benennen?**

Zu dieser Frage hat die DSK am 26. April 2018 einen Beschluss gefasst (vgl. https://www.datenschutzkonferenz-online.de/media/dskb/20180426_dskb_dsb_bestellpflicht.pdf), auf den insgesamt verwiesen wird.

Für Praxisgemeinschaften gilt, dass die einzelnen Praxen die Voraussetzungen der Benennungspflicht aufgrund ihrer rechtlichen Selbstständigkeit zwar grundsätzlich nur bezogen auf ihre eigene Praxis prüfen müssen. Sofern eine Praxisgemeinschaft allerdings ein gemeinsames Patienteninformationssystem betreibt und mindestens zehn Personen dieses ständig nutzen, kann ebenfalls eine Benennungspflicht bestehen. Da bei einem gemeinsamen Patienteninformationssystem auch eine gemeinsame Verantwortlichkeit im Sinne des Art. 26 DSGVO vorliegen kann, dürfte es sich empfehlen, jeweils dieselbe Person als Datenschutzbeauftragten zu benennen. Soll eine Person als DSB benannt werden, die nur Mitarbeiter/in in einer der Praxen ist, wäre diese Person somit teils als interner, teils als externer DSB für die Praxisgemeinschaft tätig.