Die größten Irrtümer zum Datenschutz in der Arztpraxis

Datenschutz nach Maß und ausschließlich für das Gesundheitswesen. Nutzen Sie unseren Leitfaden, um den Datenschutz für sich einfacher zu gestalten.

www.gesunder-datenschutz.de

Die größten Irrtümer in der Arztpraxis

Gesunder Datenschutz

Irrtum #1: Für die ärztliche Behandlung von Patienten muss eine Einwilligungserklärung des Patienten eingeholt werden.

Nein. Die ärztliche Behandlung wird aufgrund eines **Behandlungsvertrages** durchgeführt. Diese vertragliche Grundlage stellt eine Befugnis für die Datenverarbeitung gemäß Artikel 9 Abs. 2 Buchstabe h) und Absatz 3 in Verbindung mit Artikel 6 Absatz 1 Satz 1 Buchstabe b) Datenschutz-Grundverordnung (DSGVO) dar. Alle Verarbeitungen, die zur Erfüllung des Behandlungsvertrages notwendig sind, können auf dieser **Rechtsgrundlage** durchgeführt werden. Eine Einwilligung ist für die Verarbeitung von personenbezogenen Daten zur Erfüllung des Behandlungsvertrages daher nicht erforderlich. In die Erhebung von **Gesundheitsdaten** im Zuge einer **Anamnese** kann im Übrigen durch die Teilnahme an der Untersuchung konkludent eingewilligt werden. Die Weitergabe der Patientendaten an eine **private Abrechnungsstelle** ist –wie bisher auch– vom Behandlungsvertrag nicht abgedeckt. Hierfür ist eine entsprechende Einwilligung einzuholen.
→Grundsätzlich ist keine Einwilligung erforderlich, nur für die Weitergabe der Daten an private Abrechnungsstellen.

Irrtum #2: Ich darf als Arzt die ärztliche Behandlung verweigern, wenn der Patient nicht in die Verarbeitung personenbezogener Daten einwilligt.

Für die Verarbeitung personenbezogener Daten zum Zwecke der ärztlichen Behandlung muss grundsätzlich keine Einwilligung eingeholt werden (siehe dazu Frage 1). Die ärztliche Behandlung darf daher **auf keinen Fall** unter Berufung auf die Nichterteilung einer datenschutzrechtlichen Einwilligung **verweigert** werden.
→Folge: Ohne entsprechende Einwilligung dürfen die Patientendaten nicht an die private Rechnungsstelle weitergeleitet werden, sondern müssen in der Praxis abgerechnet werden.

Irrtum #3: Aufgrund des Grundsatzes der Datenminimierung im Verhältnis von Arzt zu Patient darf ich als Arzt bei der Anamnese nur noch die nötigsten Daten erfassen.

Aus **haftungsrechtlichen** Gesichtspunkten müssen Sie alle für die Anamnese **erforderlichen Daten** aufnehmen und auch verarbeiten!

Im Übrigen schützt die Grundrechtecharta (GRCh) der Europäischen Union in Artikel 2 Absatz 1 GRCh und Artikel 3 Absatz 1 GRCh die Rechte auf Leben und körperliche sowie geistige Unversehrtheit. Die Datenschutz-Grundverordnung ist im Lichte dieser hochrangigen Grundwerte auszulegen. Bei der ärztlichen Anamnese dürfen auch angesichts dieser Schutzgüter sämtliche personenbezogene Daten erhoben werden, die für eine fachmännische Beurteilung erforderlich sind. Bei einer nach den Regeln der Kunst durchgeführten Anamnese ist daher auch eine **Angemessenheit der Datenverarbeitung** anzunehmen.

Die größten Irrtümer in der Arztpraxis

Gesunder Datenschutz

Irrtum #4: Ein Austausch unter Ärzten ist auch unter Wahrung des Berufsgeheimnisses über medizinisch problematische Fälle nicht erlaubt.

Im Rahmen eines **Behandlungsvertrags** kann auch der Rat von **Kollegen** eingeholt werden, solange die rechtliche Befugnis aus dem (Behandlungs-)Vertragsverhältnis nicht überschritten wird. **Rechtsgrundlage** für eine Übermittlung der personenbezogenen Daten ist hier der Behandlungsvertrag nach Artikel 9 Abs. 2 Buchstabe h) und Absatz 3 in Verbindung mit Artikel 6 Absatz 1 Satz 1 Buchstabe b) DSGVO. Gemäß Artikel 14 Abs. 5 Buchstabe d) DSGVO muss der **Betroffene** vom angefragten Arzt nicht darüber informiert werden, dass Daten nicht vom Betroffenen direkt erhoben wurden, wenn die übermittelten personenbezogenen Daten dem Berufsgeheimnis unterliegen und daher vertraulich behandelt werden müssen.
→Ärztliche Fachgespräche unter Kollegen sind auch ohne Einwilligung zulässig.

Irrtum #5: Gesundheitsdaten von Patienten dürfen nicht mehr per Fax oder per E-Mail verschickt werden.

Gesundheitsdaten von Patienten sollten am besten per **Briefpost** oder mit **verschlüsselter EMail** verschickt werden.Bei der Versendung von Patientendaten per Fax ist besondere Vorsicht geboten. **Faxfehlversand** durch Wählfehler und Irrläufer sind im Zweifel meldepflichtige **Datenpannen**.

Soweit die Versendung mittels Fax aus organisatorischen Gründen geboten ist und im Einzelfall Patientendaten gefaxt werden sollen, muss beim Versenden sichergestellt sein, dass nur der Empfänger selbst oder ein ausdrücklich dazu ermächtigter Dritter Kenntnis vom Inhalt des Schreibens erhält. Dies gilt insbesondere dann, wenn ärztliche Mitteilungen an den Patienten selbst gefaxt werden.

Jeder Sendung sollte ein **Vorblatt** vorangestellt werden, welches den Absender, dessen Telefax- und Telefonnummer sowie die Anzahl der insgesamt gesendeten Seiten ausweist, sowie die deutliche Bitte, das ggf. fehlgeleitete Fax beim Absender umgehend anzuzeigen und zu vernichten, sofern man nicht der berechtigte Empfänger ist.

Welche Wege eine **E-Mail** im Internet nimmt und wer diese Kommunikation dabei zu Kenntnis nehmen kann, ist weder vom Absender noch vom Empfänger beeinflussbar. Vertrauliche Informationen wie Arztbriefe, Befunde etc. dürfen deshalb über das Internet per E-Mail nur versandt werden, wenn Maßnahmen zum Schutz vor unbefugter Kenntnisnahme ergriffen werden. Eine geeignete technische Maßnahme ist hier die Verschlüsselung. Diese ist bei Kommunikation mit externen Dritten notwendig und sollte auch bei Kontaktformularen im Internet bedacht werden. Gesundheitsdaten dürfen nicht beim Provider im Klartext vorliegen. Idealerweise wird dies mittels eines über die bloße Transportverschlüsselung hinausgehenden Schutzes, also mittels einer Ende-zu-Ende-Verschlüsselung zwischen Absender und Empfänger über die Standards GPG oder S/MIME, realisiert.
→Gesundheitsdaten am besten mit verschlüsselten E-Mails oder verschlüsselten E-Mail-Anhängen verschicken.

Die größten Irrtümer in der Arztpraxis

Irrtum #6: Die DSGVO verbietet die Datenübermittlung in die USA.

Falsch. Was die Auftragsverarbeitung betrifft, also das Verarbeiten personenbezogener Daten durch **Dienstleister**, erlaubt die DSGVO nun sogar, dass diese auch außerhalb der EU stattfinden darf. Das war zuvor nicht der Fall. Die DSGVO knüpft eine Datenübermittlung ins Nicht-EU-Ausland wie die **USA** allerdings an verschiedene Anforderungen. Dabei geht es darum, dass der Dienstleister, beispielsweise ein amerikanischer Cloud-Service, garantiert, dass das Datenschutzniveau dort demjenigen der **Europäischen Union** entspricht. Nachweisen lässt sich das etwa durch eine Zertifizierung unter dem EU-US-Privacy-Shield (zertifizierte Firmen finden sich auf der Privacy-Shield Liste) oder durch ein Datenschutz-Zertifikat nach DSGVO, das Firmen künftig erwerben können.
→Cloud-Services können eingesetzt werden, wenn sie entsprechend zertifiziert sind. Dazu beraten wir Sie gerne.

Irrtum #7: Jede Arztpraxis muss einen Datenschutzbeauftragten haben.

Nicht jede Arztpraxis ist zur Bestellung eines Datenschutzbeauftragten verpflichtet! **Allerdings muss beachtet werden, dass auch ohne einen bestellten (externen) Datenschutzbeauftragen die datenschutzrechtlichen Pflichten inkl. Dokumentation eingehalten werden. Dies schaffen die wenigsten Praxis mangels Ressourcen!**
Folgende Regelungen bestehen bei der Bestellpflicht:

1. Betreibt ein **einzelner Arzt, Apotheker oder sonstiger Angehöriger** eines Gesundheitsberufs eine Praxis, Apotheke oder ein Gesundheitsberufsunternehmen und sind dort einschließlich seiner Person in der Regel mindestens **20** Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt, besteht eine gesetzliche Verpflichtung zur Benennung eines Datenschutzbeauftragten (DSB), **außer** es besteht die Pflicht zur **Datenschutzfolgeabschätzung** (insbesondere bei Radiologen, Nuklearmedizinern, großen Praxen).

2. Bei Ärzten, Apothekern oder sonstigen Angehörigen eines Gesundheitsberufs, die zu mehreren in einer Berufsausübungsgemeinschaft **(Praxisgemeinschaft) bzw. Gemeinschaftspraxis** zusammengeschlossen sind oder die ihrerseits weitere Ärzte, Apotheker bzw. sonstige Angehörige eines Gesundheitsberufs beschäftigt haben, ist in der Regel nicht von einer umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten im Sinne von Art. 37 Abs. 1 lit. c DSGVO auszugehen – in diesen Fällen ist unter Berücksichtigung von Punkt 3 dann kein DSB zu benennen, wenn weniger als 20 Personen mit der Verarbeitung personenbezogener Daten beschäftigt sind.

3. Bei Ärzten, Apothekern oder sonstigen Angehörigen eines Gesundheitsberufs, die zu mehreren in einer Berufsausübungsgemeinschaft **(Praxisgemeinschaft) bzw. Gemeinschaftspraxis** zusammengeschlossen sind oder die ihrerseits weitere Ärzte, Apotheker bzw. sonstige Angehörige eines Gesundheitsberufs beschäftigt haben, bei denen ein **hohes Risiko für die Rechte und Freiheiten** bei der Verarbeitung personenbezogener Daten zu erwarten ist, ist eine Datenschutzfolgenabschätzung vorgeschrieben und damit zwingend ein Datenschutzbeauftragter zu benennen. Dies kann neben einer umfangreichen Verarbeitung (z.B. große Praxisgemeinschaften), die ohnehin nach Art. 37 Abs. 1 lit. c DSGVO zu einer Benennungspflicht führt, beispielsweise beim Einsatz von neuen Technologien, die ein hohes Risiko mit sich bringen, der Fall sein. Der Datenschutzbeauftragte ist damit auch dann zu benennen, 2 wenn weniger als 10 Personen ständig mit der Verarbeitung personenbezogener Daten zu tun haben.

Die größten Irrtümer in der Arztpraxis

Irrtum #8: Die DSGVO verbietet es, personenbezogene Daten in einer Cloud zu speichern.

Falsch. Personenbezogene Daten dürfen weiterhin in einer Cloud gespeichert werden – allerdings muss man mit dem Cloud-Betreiber einen Vertrag zur Auftragsverarbeitung schließen und für den gelten strengere Vorgaben als bisher. Der Cloud-Anbieter muss hinreichende Garantien dafür bieten, dass er geeignete technische und organisatorische Maßnahmen getroffen hat, die sicherstellen, dass die Datenverarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und dass die Rechte der Betroffenen gewahrt werden.
→Sie sind gem. Art. 28 DSGVO dafür verantwortlich, den Service-Anbieter anhand seiner technischen Dokumentation sorgfältig auszuwählen. Wo ist der Sitz? Werden Daten auch in Drittstaaten verarbeitet? Welche Garantien für ein angemessenes Datenschutzniveau gibt es?

Irrtum #9: Werbung ist ohne Einwilligung nicht gestattet.

Falsch. Briefwerbung ist auch für Ärzte grundsätzlich ohne Einwilligung erlaubt – auch nach der DSGVO. Hier empfiehlt es sich, einen Widerspruchshinweis in das Brieftemplate einzubinden.

Kritischer ist die Ansprache via Mail und via Telefon im Bereich des Gesundheitswesen. Insbesondere muss man hier zwischen Ansprache von Arztkollegen und Patienten unterscheiden. **Bitte lassen Sie sich bei solch einem Vorhaben dringend beraten!**
→Vorsicht bei Newletter-Werbung und „Cold Calls“ – hier fängt man sich schnell eine teure Abmahnung vom Anwalt ein.

Irrtum #10: Ich als Arzt kann selbst Datenschutzbeauftragter in meiner Praxis sein.

Falsch. Durch den innewohnenden Interessenkonflikt zwischen Ihnen als Verantwortlichen und der weisungsfreien Arbeit des Datenschutzbeauftragten dürfen Sie selbst nicht der DSB sein. **Auch nahe Angehörige dürfen diese Funktion nicht wahrnehmen!**

Die Stellung des Datenschutzbeauftragten in der Arztpraxis ist nicht einfach und oft eine zwischen den Stühlen „Effizienz“ und „Datenschutz“. Rat, Empfehlung und Anforderungen des Datenschutzbeauftragten sind der Leitung wie den Mitarbeitern oft unbequem. Es ist eine schwierige, aber auch reizvolle Aufgabe, Verfahren so zu organisieren, dass sie sowohl datenschutzgerecht als auch praktikabel sind. Die arbeitsrechtliche Stellung des Datenschutzbeauftragten entspricht der eines Betriebsrates: Die Bestellung kann nur aus einem wichtigen Grund widerrufen werden, der eine fristlose Kündigung rechtfertigen würde. Aufgabe der Praxis- oder Zentrumsleitung ist es, der Mitarbeiterschaft die positive Funktion des Datenschutzes – vor allem des **Patienten- und Mitarbeiterdatenschutzes** – zu vermitteln und dem Datenschutzbeauftragten damit eine fördernde, keine nur kritisierende Aufgabe zuzuschreiben. Die Leitung hat den Datenschutzbeauftragten nach dem Gesetz zu unterstützen, ihn ausreichend zu informieren und ihn mit den notwendigen personellen und sachlichen Kapazitäten auszustatten.
→Datenschutzbeauftragte unterstützen Sie dabei, die etwa 42 Pflichten der DSGVO einzuhalten und sind die Ansprechpartner der Aufsichtsbehörden. Daneben sorgen Datenschutzbeauftragte für die Gewährleistung der IT-Sicherheit und stehen Ihnen als Berater gerne zur Seite.

Die größten Irrtümer in der Arztpraxis

Ihre Berater bei Gesunder Datenschutz

Data Protection Counsel inkl. UK-law, Beraterin für IT-Sicherheit und Auditorin für IT-Sicherheit und Datenschutz

Lucia Ferrigno, LL.M.

In meiner Arbeit als Datenschutzjuristin und Beraterin für IT-Sicherheit verbinde ich bereits seit über 10 Jahren die Leidenschaft im Datenschutzrecht und der IT-Sicherheit zu präzisem Arbeiten, der Analyse auch komplexer Sachverhalte und die Begeisterung zur effizienten und nachhaltigen Weiterentwicklung.

Mit meinen Erfahrungen im Schnittbereich von Recht, Vertrieb, Strategie und IT-Sicherheit bringe ich schnell neue Impulse in das Unternehmen. Bei meiner Arbeit nutze ich meine Führungserfahrung und mein großes Netzwerk. Ich profitiere dabei von meiner Verhandlungskompetenz und meinen ausgeprägten Fähigkeiten, Menschen bei der Problemlösung zu begleiten. Als aufgeschlossene und humorvolle Person arbeite ich klar strukturiert, konzeptionsstark, mit Empathie und führungsmotiviert und nach Aussage meiner Mandanten macht das Datenschutzrecht mit mir sogar richtig Spaß.

Ich stehe für Umsetzungsstärke und Fokus, Integration von innovativen Ansätzen, konstruktives Feedback und wertschätzende Führung.

Die größten Irrtümer in der Arztpraxis

Rechtsanwalt für Datenschutz- und IT-Recht, Spezialist im Bereich Cyberkriminalität

Dr. Marc Maisch

Ich bin Rechtsanwalt und bereits seit über 10 Jahren auf den Gebieten des Datenschutz- und IT-Rechts tätig.

Ich berate und betreue meine überwiegend aus dem IT-Umfeld stammenden Mandanten in (beinahe allen) wirtschaftsrechtlichen Fragestellungen des Zivilrechts. Ein besonderer Beratungsschwerpunkt ist das Datenschutzrecht. Neben der praktischen Anwendung der Rechtsbereiche ist mir auch die Lehre besonders wichtig. Daher bin ich zusätzlich als Lehrbeauftragter für Datenschutzrecht an der Hochschule für den öffentlichen Dienst in Bayern, Allgemeine Innere Verwaltung, Hof tätig.

Zu meinem Leistungsportfolio gehören unter anderem die Beratung, Gestaltung und Verhandlung individueller Verträge, die Begleitung neuer Geschäftsmodelle und - sofern erforderlich - die gerichtliche Vertretung der Interessen ihrer Mandanten.

Neben meiner anwaltlichen Tätigkeit berate ich auch regelmäßig durch verschiedene TV- und Radioauftritte (z.B. beim WDR, bei Aktenzeichen XY, etc.)

Gesundheitsdatenschutz & Bußgeldrechner

www.gesunder-datenschutz.de