**FAQ – Umsetzung der Datenschutzgrundverordnung in der Arztpraxis**

## 1. Muss der Patient in die Verarbeitung der Daten in meiner Praxis einwilligen?

**NEIN,** der Patient schließt mit dem Arzt in der Regel mündlich einen Behandlungsvertrag. Um diesen zu erfüllen, muss der Arzt auch die personenbezogenen Daten des Patienten verarbeiten. Die DS-GVO erlaubt daher dem Arzt die Datenverarbeitung zur Erfüllung des Behandlungsvertrages (Art. 9 Abs. 2 lit. h DS-GVO). Alles, was Sie tun müssen, um den Behandlungsvertrag zu erfüllen, ist damit erlaubt. Dazu zählt auch die Übermittlung von Daten an mitbehandelnde Ärzte. Eine Einwilligung ist hier nicht erforderlich und sollte auch nicht vorsorglich eingeholt werden. Etwas anderes gilt nur dann, wenn der Arzt die Daten zu anderen Zwecken verarbeiten möchte (z. Bsp. um zu forschen) oder eine Verarbeitung zur Erfüllung des Behandlungsvertrages nicht mehr erforderlich ist (z. Bsp. wenn Forderungen an die privatärztliche Verrechnungsstelle abgetreten werden).

## 2. Muss ich die Patienteninformation von den Patienten unterzeichnen lassen?

**NEIN**, es genügt, wenn Folgendes beachtet wird:

- Schulung der Mitarbeiter (nebst Dokumentation), wie in der Praxis informiert werden soll. Die Patienteninformation muss vom Patienten nicht mit nach Hause bzw. zur Patientenakte genommen werden. Die Patienteninformation kann den Mitarbeitern zurückgegeben und wieder verwendet werden. Selbst ein Aushang würde genügen, wenn der Patient ausdrücklich darauf und auf die Möglichkeit hingewiesen wird, einen Ausdruck mitzunehmen.
- In der Patientenakte muss vermerkt werden, dass der Patient die Patienteninformation zur Kenntnis genommen hat. Der Vermerk kann auch nur ein Symbol, ein gesetztes Häkchen oder eine farbige Kennzeichnung sein. Es muss nur dem entsprechen, was bei der Schulung der Mitarbeiter zum Thema Information festgelegt wurde. Diese Kennzeichnung soll zudem sicherstellen, dass Patienten nicht bei jedem Besuch wiederholt auf die Information angesprochen werden, obwohl sich an der Datenverarbeitung nichts geändert hat und der Patient längst über die Information verfügt.

## 3. Muss ich die Behandlung ablehnen, wenn der Patient die Patienteninformation nicht zur Kenntnis nehmen möchte oder einer Datenverarbeitung widerspricht?

**NEIN,** die Behandlung darf nicht abgelehnt werden. Rechtsgrundlage für die Datenverarbeitung ist die Erfüllung des Behandlungsvertrages. In dieser Konstellation gibt es kein Widerspruchsrecht oder Widerrufsrecht. Lässt sich der Patient behandeln, muss er damit leben, dass seine Daten verarbeitet werden, soweit es zur Erfüllung des Behandlungsvertrages erforderlich ist. Der Patient ist andererseits natürlich nicht gezwungen, einen Behandlungsvertrag einzugehen.

## 4. Darf ich weiterhin faxen?

**JA**, es darf weiterhin gefaxt werden, obwohl es mit einem hohen Risiko verbunden ist. Schnell hat man sich vertippt und sensible Gesundheitsdaten werden unbefugten Dritten offenbart. Es gibt also kein starres Verbot und jeder Arzt sollte selbst entscheiden, ob er das Risiko eindämmen und das Faxen verantworten kann. Wir empfehlen, jedenfalls nur dann zu faxen, wenn es in der jeweiligen Situation keine zumutbaren Alternativen gibt. Dabei sollten einige Regeln beachtet werden:

- Die einzelnen Faxberichte sollten dahingehend überprüft werden, ob die richtige Nummer gewählt wurde, die Seitenanzahl stimmt und der Sendungsstatus „ok“ ist. Auf dem Faxbericht sollte mit Kennzeichnung (Häkchen) und Unterschrift auch dokumentiert werden, dass der Faxbericht überprüft wurde. Ist die Nummer falsch, der Sendungsstatus aber „ok“, hat man eine Datenpanne und es besteht akuter Handlungsbedarf.
- Die einzelnen Faxberichte sind den Patientenunterlagen beizufügen.
- Darüber hinaus sollten die Speicherplätze der Faxgeräte genutzt werden, um die Nummern von häufig angewählten Adressaten einzuspeichern. Damit lassen sich Fehler minimieren.

## 5. Darf ich weiterhin mailen?

**JA**, verschlüsselte E-Mailkommunikation ist in Ordnung – nur wird man diese häufig noch nicht sicherstellen können. Oft sind E-Mails noch „Postkarten". Der Inhalt der E-Mail ist also nicht geschützt und könnte dann von Dritten mitgelesen werden. Schon mit Blick auf das Berufsgeheimnis ist die mit unverschlüsseltem E-Mailverkehr verbundene Offenbarung von Patientendaten problematisch. Wer trotzdem im Einzelfall unverschlüsselte E-Mails versenden muss, sollte zumindest darauf verzichten, sensible Daten in der E-Mail selbst zu versenden und diese stattdessen in einem mit Passwort geschützten Anhang mitschicken. Dass Passwort – oder besser noch der Passsatz, sollte dann natürlich nicht in der E-Mail selbst mitgeschickt, sondern z. Bsp. am Telefon mitgeteilt werden. Mit regelmäßigen Empfängern kann für eine bestimmte Zeit auch ein gleichbleibender Passsatz vereinbart werden.

## 6. Sind Arbeitsunfähigkeitsbescheinigungen nach einem Jahr zwingend auch digital zu löschen?

**NEIN,** der für den Arzt bestimmte Durchschlag der Arbeitsunfähigkeitsbescheinigung ist jedoch nach einem Jahr zu löschen.

## 7. Inwieweit darf ich WhatsApp beim Arzt-Patienten-Kontakt nutzen?

Es wird dringend abgeraten, sowohl datenschutzrechtlich als auch berufsrechtlich, WhatsApp beim Arzt-Patienten-Kontakt bzw. dienstlich zu nutzen. Zur Erfüllung des Behandlungsvertrages ist die Nutzung von WhatsApp nicht erforderlich und damit auch nicht von dieser Rechtsgrundlage gedeckt. Problematisch ist bereits die bloße Nutzung von WhatsApp auf einem Gerät, mit dem Sie auch dienstliche Kontakte, etwa von Kollegen oder Patienten, verarbeiten. Haben Sie WhatsApp auf einem Mobiltelefon installiert, fragt WhatsApp Ihre Telefonkontakte ab – unabhängig davon, ob diese selbst WhatsApp-Nutzer sind. Damit übermitteln Sie diese Daten an WhatsApp. Haben Sie für diese Übermittlung keine Rechtsgrundlage, ist diese Übermittlung rechtswidrig. Wer unbedingt ein Mobiltelefon dienstlich und privat nutzen und privat auf WhatsApp nicht verzichten möchte, muss sich unbedingt technischen Rat holen, wie die Dienstkontakte auf diesem Gerät gespeichert werden können, ohne dass WhatsApp darauf Zugriff hat.

## 8. Darf ich in der Praxis weiterhin den Patienten mit Namen aufrufen?

**Ja.**
Hat ein Patient jedoch etwas dagegen, sollten sie dessen Wunsch auch respektieren und die Nennung des Namens bei diesem Patienten unterlassen.

## 9. Brauche ich einen Datenschutzbeauftragten?

In der Regel nicht. Ein Datenschutzbeauftragter für eine Arztpraxis muss bestellt werden, wenn mindestens zehn Personen ständig personenbezogene Daten automatisiert verarbeiten (vgl. § 38 Abs. 1 BDSG-neu) oder die Verarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat (§ 38 BDSG-neu, Art. 35 DS-GVO). Ein hohes Risiko kann beim Einsatz neuer Technologien oder bei der umfangreichen Verarbeitung von Gesundheitsdaten bestehen. Eine bewährte Praxisverwaltungssoftware ist keine neue Technologie in diesem Sinne. Die unabhängigen Datenschutzbehörden des Bundes und der Länder haben sich zudem darauf verständigt, dass die Verarbeitung von Gesundheitsdaten in Arztpraxen, Gemeinschaftspraxen und Praxisgemeinschaften in der Regel nicht als umfangreich anzusehen ist, wenn weniger als 10 Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind. In den meisten Fällen wird man daher davon ausgehen können, dass kleinere Arztpraxen keinen Datenschutzbeauftragten bestellen müssen.

## 10. Muss ich eine Datenschutz-Folgenabschätzung machen?

Hier verhält es sich ähnlich. Eine Datenschutz-Folgenabschätzung muss durchgeführt werden, wenn die Verarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat (Art. 35 DS-GVO). Ein hohes Risiko kann beim Einsatz neuer Technologien oder bei der umfangreichen Verarbeitung von Gesundheitsdaten bestehen. Eine bewährte Praxisverwaltungssoftware ist keine neue Technologie in diesem Sinne. Wenn weniger als 10

Personen ständig mit der Verarbeitung personenbezogener Daten in der Praxis beschäftigt sind, ist auch nicht von umfangreicher Verarbeitung von Gesundheitsdaten auszugehen. Eine Datenschutz-Folgenabschätzung wird daher regelmäßig nicht erforderlich sein. Eine Ausnahme gilt vor allem dann, wenn in der Praxis eine Verarbeitung stattfindet, die auf der sogenannten „Blacklist“ steht. Das ist eine Liste mit Datenverarbeitungen, bei denen immer eine Datenschutz-Folgenabschätzung gemacht werden muss. Eine vorläufige Blacklist hat der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern hier [https://www.datenschutz-mv.de/static/DS/Dateien/DS-GVO/Hilfsmittel%20zur%20Umsetzung/MV_DSFA_Muss-Liste.pdf] veröffentlicht. Muss eine Datenschutz-Folgenabschätzung danach durch den Arzt gemacht werden, muss er auch einen Datenschutzbeauftragten bestellen.