

RA Dr. René Sasse • Chemnitzer Straße 126 • 44139 Dortmund

Dr. René Sasse
Rechtsanwalt

Chemnitzer Str. 126
44139 Dortmund

Telefon 02 31.130 90 33
Mobil 01 76.21 05 22 46
Telefax 02 31.799 23 15

E-Mail info@rechtsanwalt-sasse.de
info@sasse-heilpraktikerrecht.de

Internet www.rechtsanwalt-sasse.de
www.sasse-heilpraktikerrecht.de

19.03.2018

Sie hatten mich gebeten, ein Merkblatt zur Datenschutzgrundverordnung (DS-GVO) für Heilpraktiker zu erstellen. Nachfolgend finden Sie eine entsprechende Auflistung für einen Einblick in die Thematik. Das Merkblatt vermittelt einen kompakten Überblick über wichtige Regelungen der DS-GVO; es erhebt jedoch keinen Anspruch auf Vollständigkeit oder umfassende bzw. vertiefte Information. Es ersetzt insbesondere keinen individuellen Rechtsrat. Je nach Art und Umfang der Praxis können weitere Punkte wichtig sein, z.B. eine sogenannte Datenschutz-Folgenabschätzung. Für weitere Informationen stehe ich gern persönlich zur Verfügung.

Für einen ersten Einblick empfehle ich zudem folgende Broschüre: Erste Hilfe zur Datenschutz-Grundverordnung für Unternehmen und Vereine; herausgegeben vom Bayerischen Landesamt für Datenschutzaufsicht; erschienen im C.H.BECK-Verlag.

Freundliche Grüße

Dr. René Sasse
(Rechtsanwalt)

Warum ist die DS-GVO so wichtig?

Die Datenschutz Grundverordnung (DS-GVO) reglementiert die elektronische Verarbeitung von personenbezogenen Daten. Da in jeder Heilpraktikerpraxis (Patienten-)Daten in elektronischer Form erhoben, verarbeitet und ggfs. weitergeleitet werden, sind diese Vorgaben wichtig. Beispiele für eine Datenverarbeitung sind z.B.

- eine elektronische Patientenkartei,
- die Nutzung einer Abrechnungssoftware,
- die Praxishomepage,
- Email-Korrespondenz, Nutzung eines Kontaktformulars.

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, beispielsweise Name, Anschrift, E-Mail-Adresse. Wichtig: Die DS-GVO betrachtet gesundheitsbezogene Daten als besonders schutzwürdig. Da Heilpraktiker solche Daten verarbeiten, ist große Sorgfalt geboten. Bei Verstößen drohen empfindliche Bußgelder, Schadensersatzansprüche oder Abmahnungen durch Mitbewerber oder Wettbewerbsverbände.

Ab wann gilt die DS-GVO?

Die DS GVO gilt ab dem 25. Mai 2018.

Was sind die wichtigsten Maßnahmen, um die Vorgaben der DS-GVO zu erfüllen?

Erstellen Sie ein Verarbeitungsverzeichnis. Nach Art. 30 DS-GVO müssen alle Verantwortlichen ein Verzeichnis über sämtliche Verarbeitungstätigkeiten führen, die in ihrem Unternehmen durchgeführt werden. Es muss dort dokumentiert werden, in welchem Zusammenhang mit personenbezogenen Daten gearbeitet wird. Verantwortlich hierfür ist der Heilpraktiker als Praxisinhaber; dieser haftet bei Verstößen gegen diese Vorgabe.

Unternehmen, die weniger als 250 Mitarbeiter beschäftigen, müssen eigentlich kein Verarbeitungsverzeichnis führen. Allerdings gilt diese Ausnahmeregelung nicht für Unternehmen, die gesundheitsbezogene Daten verarbeiten. Da Heilpraktiker gesundheitsbezogene Daten verarbeiten, muss hier stets ein Verarbeitungsverzeichnis in der Praxis geführt werden. Zudem dürften auch andere Firmen mit weniger als 250 Mitarbeitern in der Regel verpflichtet sein, ein Verarbeitungsverzeichnis zu führen, weil die Ausnahmeregelung noch an weitere Bedingungen geknüpft ist, welche in der Praxis nur selten erfüllt werden. So setzt die Ausnahmeregelung insbesondere voraus, dass die Daten nur gelegentlich verarbeitet werden. Ein Verein, der seine Mitgliederverwaltung stetig aktualisiert, ist deshalb von der Freistellung bereits nicht mehr umfasst und benötigt ein Verarbeitungsverzeichnis. Gleiches gilt für Heilpraktikerschulen.

Das Verarbeitungsverzeichnis ist in deutscher Sprache zu führen. Die Dokumentation kann schriftlich oder elektronisch erfolgen. Da das Verzeichnis stets aktuell sein muss, ist es regelmäßig zu aktualisieren und bei Veränderungen anzupassen. Eine Versionierung ist ratsam.

Nach Art. 30 Abs. 1 DS-GVO muss das Verzeichnis folgende Punkte umfassen:

- *den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;*

- die Zwecke der Verarbeitung;
- eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
- die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
- wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

Zu empfehlen ist, dass ferner die jeweiligen Verarbeitungstätigkeiten konkret beschrieben und die einschlägigen Rechtsgrundlagen festgehalten werden. Auf diese Weise schafft das Verzeichnis Klarheit, welche Datenverarbeitungsprozess in der Praxis ablaufen und ob diese rechtmäßig sind. Sofern Sie einmal eine gute Vorgehensweise erarbeitet haben, können Sie diese grundsätzlich unbefristet fortsetzen. Beachten Sie: Eine Datenübertragung ins Ausland erscheint auf den ersten Blick abwegig, aber was gilt bei Nutzung von Facebook, WhatsApp oder Cloud-Diensten?

Wie erstelle ich ein Verarbeitungsverzeichnis?

Einzel-Heilpraktikerpraxen können sich grundsätzlich an Mustern orientieren, die von den Aufsichtsbehörden im Internet kostenlos angeboten werden. Ratsam ist auch der Besuch von günstigen Webinaren und die Lektüre von Informations-Broschüren. Die Datenschutzkonferenz (DSK) veröffentlicht Auslegungshilfen zur Datenschutz-Grundverordnung (DS-GVO). Diese Kurzpapiere geben weitere Hilfestellungen. Sie sind im Internet über die Landesbeauftragten für den Datenschutz abrufbar, z.B. <https://www.datenschutz-hamburg.de/news/detail/article/kurzpapiere-der-dsk-zur-dsgvo.html>

Sofern jedoch komplexere Datenverarbeitungen erfolgen, sollte ein externer Rat bei einem Anwalt oder Datenschutzberater eingeholt werden. Dies gilt vor allem auch für Heilpraktiker, die sich zur gemeinsamen Berufsausübung zusammengeschlossen haben (Gemeinschaftspraxen). Das Verarbeitungsverzeichnis ist zentraler Bestandteil des Datenschutzkonzepts jeder Heilpraktikerpraxis. Die Aufsichtsbehörden können jederzeit die Vorlage des Verarbeitungsverzeichnisses verlangen. Kann dieses nicht unverzüglich vorgelegt werden, droht ein Bußgeld in empfindlicher Höhe.

Was ist bei der Datenschutzerklärung für meine Praxishomepage zu beachten?

Bereits bislang haben Sie für Ihre Praxiswebsite eine Datenschutzerklärung benötigt. In dieser Erklärung ist über die Erhebung personenbezogener Daten bei Nutzung der Internetpräsenz zu informieren. Die DS-GVO stellt hier nochmals konkretere Anforderungen als die bisherige Rechtslage. Insbesondere ist zukünftig eine konkrete Rechtsgrundlage für die jeweilige Datenverarbeitung anzugeben, zudem ist die verantwortliche Stelle konkret zu bezeichnen. Insgesamt ist die Datenschutzerklärung zukünftig konkreter und somit auch ausführlicher zu halten. Sofern statistische Analysetools oder Plugins sozialer Onlineplattformen genutzt werden,

ist eine umfassende Information erforderlich. Letztlich bedarf die überwiegende Vielzahl der aktuellen Datenschutzerklärungen einer Anpassung.

Aufgrund dieser Änderungen sollte jeder Heilpraktiker seine Datenschutzerklärung auf einen etwaigen Anpassungsbedarf überprüfen. Da die Datenschutzerklärung im Internet frei zugänglich sein muss, droht diesbezüglich eine erhebliche Abmahngefahr durch Wettbewerbsverbände oder Mitbewerber, sofern diese Erklärung nicht rechtskonform gestaltet ist. Zudem drohen Sanktionen durch die Aufsichtsbehörden, weil entsprechende Verstöße sehr leicht aufzudecken sind.

Mitglieder Ihres Verbandes können das Muster „Datenschutzerklärung“ verwenden, welches ich in Ihrem Auftrag erstellt habe.

Prüfen Sie, ob Daten rechtskonform erhoben und verarbeitet werden!

Personenbezogene Daten dürfen vom Heilpraktiker ausschließlich dann erhoben, gespeichert oder weitergegeben werden, wenn hierfür eine Einwilligung des Patienten oder ein gesetzlicher Rechtfertigungsgrund vorliegt. (Prinzip des Verbots mit Erlaubnisvorbehalt).

Für Heilpraktiker gilt: Die Verarbeitung personenbezogener Daten ist nur dann rechtlich zulässig, sofern

- die hiervon betroffene Person (insbesondere der Patient) eine Einwilligung hierzu erteilt hat,
- die Verarbeitung für die Erfüllung eines Vertrages oder einer rechtlichen Verpflichtung erforderlich ist
- oder die Verarbeitung zur Wahrung der berechtigten Interessen des Heilpraktikers oder eines Dritten erforderlich ist und nicht die Interessen der betroffenen Person überwiegen.

Prüfen Sie vor jeder Datenerhebung, Datenverarbeitung oder Datenweitergabe, ob hierfür eine Rechtsgrundlage besteht. Ist dies nicht der Fall, ist der Vorgang rechtswidrig und kann empfindliche Bußgelder zur Folge haben.

Bitte beachten Sie, dass das Gesetz hohe Anforderungen an die Einwilligung des Betroffenen stellt. Diese sind bei der Einholung der Einwilligung einzuhalten. Der Passus „Wahrung berechtigter Interessen des Verantwortlichen“ ist vage gehalten und kann in der Praxis zu schwierigen Abgrenzungsfragen führen. Problematisch ist z.B. die Nutzung eines Kontaktformulars auf der Praxishomepage.

Erfüllt die Datenverarbeitung diese Kriterien, sind weitere Grundsätze zu beachten. Hierbei handelt es sich insbesondere um die „Zweckbindung der Verarbeitung“, d.h. die Verarbeitung darf ausschließlich für die konkret festgelegten Zwecke erfolgen. Weitere Grundsätze sind z.B. die „Richtigkeit der Daten“, die „Erforderlichkeit der Speicherung“ und die „Rechenschaftspflicht“.

Wichtig: Zukünftig müssen Sie die Datenschutzvorgaben nicht nur einhalten; sie müssen deren Beachtung darüber hinaus auch gegenüber den Aufsichtsbehörden nachweisen können. Hierzu ist eine Dokumentation in schriftlicher oder elektronischer Form erforderlich. Hier bietet sich eine Ergänzung des Verarbeitungsverzeichnisses an.

Was ist eine Auftragsverarbeitung?

Sofern Sie als Heilpraktiker eine andere Stelle (Unternehmen) heranziehen, um personenbezogene Daten in Ihrem Auftrag verarbeiten zu lassen, spricht man von einer Auftragsverarbeitung. In diesem Fall übermitteln Sie personenbezogene Daten an einen

Außenstehenden - also an eine Person, die nicht Ihrer Praxis angehört. Eine Auftragsverarbeitung findet zum Beispiel in folgenden Fällen statt:

- Wartung Ihrer Praxis-EDV durch externe IT-Dienstleister
- Nutzung einer Online-Abrechnungssoftware
- Cloud-Computing
- Adressweitergabe an einen Lettershop, z.B. für Weihnachtsgrußkarten

In diesen Fällen ist ein so genannter Auftragsverarbeitungsvertrag mit dem jeweiligen Anbieter zu schließen. Ohne einen solchen Vertrag ist die Datenweitergabe rechtswidrig oder bedarf der konkreten Einwilligung der betroffenen Personen. Abzugrenzen ist die Auftragsverarbeitung von der Inanspruchnahme externer Fachleistungen (z.B. Rechtsanwalt, Steuerberater).

IT-Sicherheit & Datenverfügbarkeit

Die IT-Sicherheit ist ein Punkt, mit dem sich jeder Heilpraktiker befassen muss. Bislang wurde die IT-Sicherheit leider oftmals nur stiefmütterlich behandelt. Sie sind jedoch nunmehr gesetzlich verpflichtet, sich gegen mögliche Risiken und Gefahren in der IT-Welt zu wappnen. Dies betrifft sowohl Gefahren von Hacking-Attacken, als auch Risiken eines ungewollten Datenverlusts. Die Vertraulichkeit der Daten ist zu wahren.

Die DS-GVO nennt in Art. 32 folgende Schutzziele:

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Sie müssen Sorge tragen, dass die bei Ihnen gespeicherten Daten bei Bedarf genutzt werden können, also verfügbar sind. Das Erstellen regelmäßiger Datensicherungen (Backups) ist rechtlich geboten. Ein Konzept zur IT-Sicherheit ist eine rechtliche Pflicht, für deren Einhaltung der Praxisinhaber verantwortlich ist. Hierbei sind auch diese Punkte zu berücksichtigen: Nutzung von E-Mails, WLAN-Netzen, mobilen Endgeräten.

Datenschutzbeauftragter

Benötigen Heilpraktikerpraxen einen Datenschutzbeauftragten? Diese Frage erzeugt momentan erhebliche Rechtsunsicherheit. Ein Datenschutzbeauftragter unterstützt den eigentlich Verantwortlichen in Fragen des Datenschutzes.

Sofern in Ihrer Praxis mindestens zehn Personen vorhanden sind, die personenbezogene Daten verarbeiten, benötigen Sie in jedem Fall einen Datenschutzbeauftragten. Dies dürfte jedoch bei den wenigsten Heilpraktikern der Fall sein. Allerdings kann ein Datenschutzbeauftragter auch dann erforderlich sein, wenn zwar weniger als zehn Personen mit der Datenverarbeitung betraut sind, jedoch (besonders schutzwürdige) Gesundheitsdaten verarbeitet werden. Diese Voraussetzung ist in der Heilpraktikerpraxis erfüllt. Weitere Voraussetzung ist jedoch, dass die Verarbeitung von diesen Daten umfangreich ist und eine Kerntätigkeit des Heilpraktikers darstellt. Die Auslegung dieses Passus ist noch nicht abschließend geklärt, sodass Unsicherheiten verbleiben. Im Zweifelsfalle sollte die Datenschutzbehörde angefragt werden. Die Verarbeitung personenbezogener Daten gilt nicht als umfangreich, wenn sie die Verarbeitung personenbezogener Daten von Patienten betrifft und durch einen einzelnen Angehörigen eines Gesundheitsberufes erfolgt. Einzelheilpraktiker benötigen demnach in der Regel keinen Datenschutzbeauftragten. Bei Gemeinschaftspraxen mit weniger als 10 Beschäftigten bleiben aktuell Fragen offen.

Was sind Betroffenenrechte?

Personen, deren Daten verarbeitet werden, haben konkrete Rechte. Beispielsweise das Recht auf transparente Information. Sofern Sie personenbezogene Daten von Patienten verarbeiten, müssen Sie diese in präziser transparenter und verständlicher sowie leicht zugänglicher Form in einer klaren und einfachen Sprache darüber informieren, was zu welchem Zweck mit den Daten gemacht werden soll. Um diese Pflicht zu erfüllen sollte ein Merkblatt als Anlage zum Behandlungsvertrag verwendet werden.

Nach Art 13 DS-GVO gilt im Einzelnen:

Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:

- *den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;*
- *gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;*
- *die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;*
- *wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;*
- *gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten*
- *gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.*

Zusätzlich zu diesen Informationen stellt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen zur Verfügung, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:

- *die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;*

- das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;
- wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte;
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Diese umfassende Informationserteilung dürfte von vielen Heilpraktikern als formelle Zumutung empfunden werden. Im Praxisalltag dürfte eine strikte Erfüllung dieser Pflicht so manche Stilblüte nach sich ziehen. Wichtig ist aber: Nehmen Sie diese Vorgabe dennoch ernst! Verwenden Sie ein Merkblatt, um diese Pflicht im Praxisalltag zu erfüllen.

Mitglieder Ihres Verbandes können das Muster „Informationspflichten“ verwenden, welches ich in Ihrem Auftrag erstellt habe.

Auskunftsrecht

Sofern Sie von Patienten personenbezogene Daten gespeichert haben, müssen Sie diesen die Daten ggfs. zukommen lassen: Nach Art. 15 DS-GVO gilt:

Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf folgende Informationen:

- die Verarbeitungszwecke;
- die Kategorien personenbezogener Daten, die verarbeitet werden;
- die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;
- falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
- das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige

*Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.
→ Werden personenbezogene Daten an ein Drittland oder an eine internationale Organisation übermittelt, so hat die betroffene Person das Recht, über die geeigneten Garantien gemäß Artikel 46 im Zusammenhang mit der Übermittlung unterrichtet zu werden.*

Bereiten Sie sich auf entsprechende Auskunftersuchen von Patienten vor! Wenn Sie diese Auskunftspflichten nicht rechtzeitig erfüllen können, kann sich der Betroffene bei der Aufsichtsbehörde beschweren. In diesem Fall droht eine Sanktion.

Sanktionen

Wichtig: Datenschutz ist Patientenschutz und sollte deshalb „freiwillig“ erfolgen. Zu einem professionellen Arbeiten zählt ein guter Schutz der Patientendaten. Ein Datenschutz rein aus Furcht vor Bußgeldern ist meist nicht hilfreich und führt oft zu Fehlern in der Handhabung. Es ist aber wichtig, die möglichen Sanktionen zu kennen.

Die DS-GVO ermächtigt die Datenschutzaufsichtsbehörden bei Verstößen gegen diese Verordnung Geldbußen in einer Höhe von bis zu 20 Millionen € festzusetzen, bei Unternehmen alternativ Geldbußen von bis zu 4 % des Weltjahresumsatzes. Zudem drohen Abmahnungen durch Wettbewerbsverbände oder Mitbewerber. Insgesamt ist ein schärferes Einschreiten der Aufsichtsbehörden zu erwarten. Die Geldbußen sollen in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein. Auch Heilpraktiker, kleine Unternehmen oder kleine Vereine müssen deshalb mit empfindlichen Bußgeldern rechnen. Bei gravierenden Verstößen sind Bußgelder in vier- oder fünfstelliger Höhe möglich.

Jede Person, der wegen eines Verstoßes gegen die DS-GVO ein materieller oder immaterieller Schaden entstanden ist, hat zudem Anspruch auf Schadensersatz (Art. 82 Abs. 1 DS-GVO). Wird beispielsweise versehentlich der Befund eines Patienten per Fax oder Email an Außenstehende übermittelt, droht ein hohes Schmerzensgeld.

Hinweis: Dieses Merkblatt vermittelt einen kompakten Überblick über wichtige Regelungen der DS-GVO; es erhebt jedoch keinen Anspruch auf Vollständigkeit oder umfassende bzw. vertiefte Information. Je nach Art des Unternehmens können weitere Punkte wichtig sein, z.B. eine sogenannte Datenschutz-Folgenabschätzung. Für weitere Informationen empfehle ich folgende Broschüre: Erste Hilfe zur Datenschutz-Grundverordnung für Unternehmen und Vereine; herausgegeben vom Bayerischen Landesamt für Datenschutzaufsicht; erschienen im C.H.BECK-Verlag.