Thieme

Datenschutzgrundverordnung (DSGVO) – Schreckgespenst oder echte Bedrohung?

Sylke Wagner-Burkard

Die Datenschutzgrundverordnung (DSGVO) wurde mit Ablauf der Übergangsfrist am 25.5.2018 direkt geltendes Recht, sie ist in jedem EU-Mitgliedstaat unmittelbar wirksam und geht nationalem Recht vor. Ziel dieser „Durchgriffswirkung" ist die Einheitlichkeit des Datenschutzrechts in allen EU-Ländern.

Da das deutsche Datenschutzrecht zuvor ohnehin eines der strengsten Datenschutzrechte Europas war, sind die Änderungen für die Betroffenen im Gegensatz zu anderen europäischen Ländern nicht gravierend. Allerdings ist der Datenschutz nun in Deutschland aus dem Bereich der Grauzone herausgetreten und wird ernst(er) genommen, wohl auch wegen der erheblichen Sanktionsmöglichkeiten von bis zu 20 Mio. Euro oder 4% des Gesamtumsatzes des Unternehmens.

Umsetzung in einer osteopathischen Praxis

Jeder Inhaber einer osteopathischen Praxis ist ein „Verantwortlicher" im Sinne der DSGVO (Art. 4 Nr. 7 DSGVO), da in der Praxis „personenbezogenen Daten" verarbeitet werden. Hierbei ist zu beachten: Nach Art. 4 Nr. 1 DSGVO ist jede Information über eine natürliche Person ein personenbezogenes Datum. Als natürliche Person kommt in der osteopathischen Praxis Patienten und Mitarbeiter in Betracht.

Merke

Es gibt keine Praxis, die keine personenbezogenen Daten erhebt, speichert oder auf eine andere Art damit umgeht. Jeder Umgang mit den Daten ist eine „Verarbeitung" im Sinne der DSGVO (Art. 4 Nr. 2 DSGVO). Das bedeutet: Ausnahmslos jede Praxis ist zur Umsetzung der DSGVO verpflichtet.

1. Schritt: Datenschutzgrundsätze beachten

Daten müssen unabhängig von der berufsrechtlichen Tätigkeitsbefugnis des Therapeuten auf Basis einer datenschutzrechtlichen Rechtsgrundlage verarbeitet werden (Grundsatz der Rechtmäßigkeit). Dafür kommen regelmäßig 3 Rechtsgrundlagen in Betracht:

- **Einwilligung der betroffenen Person** (Art. 6 Abs. 1 lit. a DSGVO): Beispiel: Ein Patient erhält regelmäßig einen Newsletter, in dem er über Dinge rund um die Praxis und Therapierichtung informiert wird und weitere Dienste der Praxis angeboten werden.
- **Verarbeitung zur Umsetzung eines Vertrags** (Art. 6 Abs. 1 lit. b DSGVO) **bzw. Behandlungsvertrags** (Art. 9 Abs. 2 lit. h DSGVO): Beispiel: Der Kunde eines Yoga-Studios bucht einen Yoga-Kurs. Für Buchung, Abwicklung und Berechnung des vereinbarten Preises benötigt das Yoga-Studio keine Einwilligung des Kunden, das Datenschutzrecht erlaubt dies auf Basis des Art. 6 Abs. 1 lit. b DSGVO.
- **Verarbeitung zur Wahrung eines berechtigten Interesses nach Interessenabwägung** (Art. 6 Abs. 1 lit. f DSGVO): Beispiel: Der Besucher der Webseite hinterlässt dabei personenbezogene Daten, auch ohne konkreten Eintrag in ein Kontaktformular. Die Verarbeitung dieser Daten durch den Webseiteninhaber zur Ermöglichung des Besuchs erfolgt auf Basis eines berechtigten Interesses nach Art. 6 Abs. 1 lit. f DSGVO. Ein überwiegendes entgegenstehendes Interesse des Besuchers besteht nicht, sodass die Datenverarbeitungen zulässig sind. Dies kann allerdings anders aussehen, wenn sog. Tracking Tools verwendet werden, durch die das Besuchsverhalten des Besuchers analysiert wird.

Entgegen vieler Gerüchte bedarf also auch nach der DSGVO **nicht jede Datenverarbeitung** der **Einwilligung der betroffenen Person**, denn, wie beispielhaft aufgezeigt, erlaubt die DSGVO bei der Verarbeitung zur Umsetzung eines Vertrags die Datenverarbeitung auch ohne Einwilligung.

Problematisiert wurde die Frage, ob nach Art. 9 Abs. 2 lit. h DSGVO auch die Datenverarbeitung zum Zweck der Umsetzung des **Behandlungsvertrags** zwischen dem **Patienten** und **dem Heilpraktiker** zulässig ist. Nach Art. 9 Absatz 3 des DSGVO wird verlangt, dass der Behandler einem Berufsgeheimnis unterliegt oder sonst nach nationalem Recht oder Unionsrecht einer Geheimhaltungspflicht unterliegt. Der Heilpraktiker ist zwar kein Berufsgeheimnisträger, unterliegt allerdings doch einer zivilrechtlichen Geheimhaltungspflicht. Aus diesem Grund hält die Mehrzahl der angefragten Landesaufsichtsbehörden Datenverarbeitungen zur Umsetzung des Behandlungsvertrags durch einen Heilpraktiker nach Art. 9 Abs. 2 lit. h DSGVO für zulässig, sodass eine zusätzliche Einwilligung des Patienten hierfür nicht erforderlich ist. Eine einheitliche Position haben die Aufsichtsbehörden dazu leider aber bislang nicht eingenommen. Rechtssicherheit ist daher nur durch eine Anfrage bei der für die jeweilige Praxis zuständigen Landesaufsichtsbehörde zu erhalten (s. zu den zuständigen Behörden www.was-ist-datenschutz.de/fuer-betroffene/aufsichtsbehoerden-datenschutz-in-deutschland.html).

Die Verarbeitung der Daten darf nur zu dem jeweiligen Zweck der Datenverarbeitung erfolgen **(Grundsatz der Zweckgebundenheit).** Wenn beispielsweise die Daten zur Umsetzung eines Vertrags verarbeitet werden, dürfen diese nicht ohne Weiteres zur Versendung von Newslettern genutzt werden. Hierfür bedarf es dann einer weiteren Rechtsgrundlage, z. B. der Einwilligung des Patienten. Ferner dürfen

Dieses Dokument wurde zum persönlichen Gebrauch heruntergeladen. Vervielfältigung nur mit Zustimmung des Verlages.

auch nur die Daten genutzt werden und nur in dem Maße, wie es die zur Erreichung des jeweiligen Zwecks erforderlich ist **(Grundsatz der Datenminimierung).** Der Praxisinhaber muss auch Maßnahmen vorsehen, die sicherstellen, dass nicht korrekte personenbezogene Daten korrigiert oder gelöscht werden **(Grundsatz der Richtigkeit)** und die Speicherung darf nur solange erfolgen, wie dies für die Erreichung des Zwecks erforderlich ist **(Grundsatz der Speicherbegrenzung).** Diesem Grundsatz steht das Recht der betroffenen Person auf Löschung gegenüber. Die personenbezogenen Daten müssen also mit Zweckerreichung gelöscht werden, wenn keine dem entgegenstehenden Aufbewahrungspflichten die Aufbewahrung erforderlich machen.

Weiterhin müssen angemessene technische und organisatorische Maßnahmen (TOM) zur Sicherstellung der Integrität und Vertraulichkeit der Nutzung umgesetzt werden **(Grundsatz der Integrität und Vertraulichkeit).**

Neu ist die **Rechenschaftspflicht** der Praxis nach Art. 5 Abs. 2 DSGVO: Die verantwortliche Stelle muss also nachweisen, dass sie die Datenschutzgrundsätze umsetzt. Kann sie dies nicht, verletzt sie die Nachweispflicht nach Art. 5 Abs. 2 DSGVO und es drohen empfindliche Sanktionen (Art. 83 Abs. 5 Nr. a DSGVO).

2. Schritt: Informationspflichten erfüllen

Nach Art. 13 und 14 DSGVO ist die verantwortliche Stelle verpflichtet, die betroffene Person u. a. über den Zweck der Verarbeitung, die verarbeiteten Daten, Empfänger der Daten und die Rechte der betroffenen Person zu informieren.

Diese Information muss nach dem Wortlaut Art. 13 Abs. 1 DSGVO „zum Zeitpunkt der Erhebung dieser Daten“ erfolgen. Das würde bedeuten, dass ein Patient bei der telefonischen Kontaktaufnahme mit der Praxis, die dazu führt, dass Name und Kontaktdaten in den Kalender der Praxis eingetragen werden, zuvor informiert werden müsste. Dies ist nicht handhabbar, was auch die Aufsichtsbehörden eingesehen haben. Nach einer Umfrage bei den Landesaufsichtsbehörden hat sich daher folgende Empfehlung herauskristallisiert:

- Den Praxen wird empfohlen, einen **Flyer** oder ein **Infoblatt** mit den entsprechenden Informationen in der Praxis bereit zu halten und dieses jedem Patienten einmalig zur Verfügung zu stellen, wenn dieser die Praxis aufsucht.
- Hierüber ist in der jeweiligen Patientenakte ein kurzer Vermerk zu machen, sodass die Erfüllung der **Informationspflicht dokumentiert** ist. In Ergänzung, aber nicht als alleinige Maßnahme, wird auch ein Aushang in der Praxis empfohlen sowie ein Verweis auf einen Datenschutzhinweis auf der Webseite der Praxis.
- Eine proaktive Information sämtlicher „Alt-Patienten“ ist nicht erforderlich.

Als Checkliste für die Gestaltung des Infoblatts kann die folgende Auflistung von Fragen dienen, die uneingeschränkt beantwortet werden müssen:

- Wer ist der Verantwortliche und ggf. sein Vertreter (in der osteopathischen Praxis ist dies der Praxisinhaber)?
- Wer ist der Datenschutzbeauftragte (wenn ein solcher zu benennen ist)?
- Welche Daten werden verarbeitet?
- Welche Zwecke werden mit der Datenverarbeitung verfolgt?
- Auf welcher Rechtsgrundlage wird verarbeitet?
- Wie lange werden die Daten gespeichert? Oder welche Kriterien werden für die Dauer zugrunde gelegt?
- Werden die Daten an Dritte (Empfänger) weitergegeben, beispielsweise an ein Steuerbüro, ein privates Abrechnungsunternehmen?
- Werden Daten außerhalb der EU verarbeitet, beispielsweise durch die Nutzung eines in der USA ansässigen E-Mail-Anbieters?
- Wenn ja, wo und durch wen und wie ist das angemessene Datenschutzniveau gewährleistet?
- Wenn Daten auf Basis einer Einwilligung verarbeitet werden, wird auf das Widerrufsrecht hingewiesen?
- Wenn Daten auf Basis einer Interessenabwägung verarbeitet werden, wie ist das berechtigte Interesse des Verantwortlichen? Wie am Beispiel des Newsletters erläutert, wäre das berechtigte Interesse in diesem Fall die Information des Patienten über Neues rund um die Praxis.
- Wird die betroffene Person über ihr Recht auf Auskunft, auf Berichtigung oder Löschung, Einschränkung der Verarbeitung, das Widerspruchsrecht gegen die Verarbeitung sowie das Recht auf Datenübertragbarkeit informiert?
- Informiert der Praxisinhaber über das Recht auf Beschwerde bei der Aufsichtsbehörde?
- Wenn Daten von der betroffenen Person selbst angegeben werden: Weise ich darauf hin, ob eine vertragliche oder gesetzliche Verpflichtung zur Angabe der Daten besteht und ob dies für den Vertragsschluss erforderlich ist und welche Konsequenzen es hat, wenn keine Daten angegeben werden? Bestellt der Betroffene beispielsweise durch Angabe seiner Daten einen Newsletter, ist darauf hinzuweisen, dass es zur Angabe der Kontaktdaten keine rechtliche oder gesetzliche Verpflichtung gibt, die Versendung des Newsletters aber ohne diese Daten nicht möglich ist.
- Wenn ein Verfahren über eine automatisierte Entscheidungsfindung (z. B. Profiling) zum Einsatz kommt: Welche Logik wird hierbei verfolgt und welche Tragweite und Wirkungen hat diese Art der Verarbeitung?
- Wenn Daten von Dritten erhoben werden, beispielsweise Kontaktdaten von potenziellen Interessierten für die eigene osteopathische Praxis von einem Dritten erworben werden: Aus welcher Quelle stammen die Daten, ggf. aus öffentlich zugänglichen Quellen?

Merke

Datenschutzerklärung auf der Webseite nicht vergessen. Die genannten Informationspflichten gelten ebenfalls für die Webseiten. Hier ist die betroffene Person nicht der Patient bzw. der Mitarbeiter, sondern der Besucher der Webseite, der über die Datenverarbeitungen, die beim Besuch der Webseite stattfinden, informiert werden muss.

Jede Webseite verarbeitet personenbezogene Daten und benötigt eine Datenschutzerklärung, auch wenn keine Möglichkeit für den Besucher besteht, selbst

Dieses Dokument wurde zum persönlichen Gebrauch heruntergeladen. Vervielfältigung nur mit Zustimmung des Verlages.

Daten – beispielsweise in einem Kontaktformular – anzugeben. Grund ist, dass auch die IP-Adressen, die bei jedem Besuch einer Webseite erhoben werden, personenbezogene Daten darstellen.

Die Datenverarbeitungen auf den Webseiten erfolgen häufig auch durch das Setzen von Cookies. Diese Textdateien enthalten Informationen, die es einem Webserver ermöglichen, einen Anwender wiederzuerkennen und Einstellungen zu speichern. Entscheidend ist, welcher Zweck mit diesen Cookies verfolgt wird; hierauf muss der Besucher der Webseite hingewiesen werden. Dies gilt auch für die Einbindung anderer Dienste, wie z. B. von bestimmten Tools zur Datenverkehrsanalyse von Webseiten (Matomo, Google-Analytics) oder dem Einbinden von Schriftformen, z. B. google fonts, auf der Webseite. All diese Dienste gehen mit dem Verarbeiten von Daten einher, über die der Webseitenbetreiber als Verantwortlicher im Sinne des Datenschutzrechts den Besucher der Praxiswebseite informieren muss.

Merke

Kommunizieren Sie gut mit Ihrem Webseitenprovider und finden Sie heraus, welche Datenverarbeitungen wirklich auf der Webseite erfolgen.

Häufig ist dem Betreiber der Seite gar nicht bekannt, welche Datenverarbeitungswerkzeuge der Webseitenersteller eingebaut hat, wodurch ein hinreichender Datenschutzhinweis unmöglich wird.

Der Hinweis muss deutlich erkennbar als Datenschutzhinweis auf der Hauptseite und jeder Unterseite einsehbar sein – bitte nicht unter „Impressum“ anbringen, sondern immer mit extra Button „Datenschutz“ oder „Datenschutzhinweis“.

3. Schritt: Datenverarbeitungsverzeichnis erstellen

Die Praxisinhaber müssen nach Art. 30 DSGVO ein sog. Datenverarbeitungsverzeichnis führen. Darin müssen Angaben gemacht werden über den Verantwortlichen, die Zwecke der Verarbeitung, die Kategorie der betroffenen Personen und der personenbezogenen Daten sowie die Empfänger der Daten. Für die Bearbeitung von Patientendaten bedeutet dies, dass angegeben werden muss, dass personenbezogene Daten wie Kontaktdaten, Gesundheitsdaten zum Zwecke der Umsetzung des Behandlungsvertrags verarbeitet werden und die betroffene Person der Patient ist. Der Steuerberater und ggf. ein privates Abrechnungsunternehmen müssen als Empfänger benannt werden. Es muss angegeben werden, ob Daten in ein sog. Drittland außerhalb der EU übermittelt werden, welche Fristen für die Löschung der Daten und welche technischen und organisatorischen Maßnahmen der Datensicherheit bestehen. Es empfiehlt sich, das Verzeichnis in Form einer Tabelle zu führen, aufbauend auf der ersten Spalte „Verarbeitungszweck“, dann eine Information über die Kategorie der betroffenen Personen (Beispiel: Patienten) und über die betroffenen Kategorien der Daten (Beispiel: Kontaktdaten, Gesundheitsdaten) etc. In die Übersicht sind keine Namen der Patienten aufzunehmen. Es soll der Aufsichtsbehörde lediglich im Falle einer Prüfung die Möglichkeit gegeben werden, sich einen Überblick über alle Datenverarbeitungsprozesse der Praxis zu machen. Das Nicht-Führen eines Verzeichnisses wird ebenfalls streng sanktioniert.

4. Schritt: Mitarbeiter und Auftragsverarbeiter verpflichten

Die Mitarbeiter müssen auf die Datenschutzvorschriften verpflichtet werden. Auch sog. Auftragsdatenverarbeiter, die

Anzeige

Dieses Dokument wurde zum persönlichen Gebrauch heruntergeladen. Vervielfältigung nur mit Zustimmung des Verlages.

Zugang zu den personenbezogenen Daten haben (z. B. privates Abrechnungsunternehmen), sind auf die Datenschutzvorschriften in einem gesonderten Vertrag zu verpflichten. Bei den jeweiligen Aufsichtsbehörden gibt es hierzu mittlerweile gute Muster, mit denen sich auch die Praxisinhaber behelfen können (z. B. Bayrisches Landesamt für Datenschutzaufsicht unter www.lda.bayern.de/de/datenschutz_eu.html).

5. Schritt: Datenschutzbeauftragten bestellen

Ein Datenschutzbeauftragter ist erforderlich, wenn mindesten 10 Personen in der Praxis mit der automatisierten Verarbeitung von personenbezogenen Daten beschäftigt sind. Das wäre z. B. der Fall, wenn mindestens 10 Personen in der Praxis Zugang zu den personenbezogenen Daten in der Praxissoftware haben und dort Einträge tätigen. Der Praxisinhaber wird nach herrschender Ansicht hierbei mitgezählt.

Nach Art. 37 DSGVO ist ein Datenschutzbeauftragter auch dann erforderlich, wenn die Verarbeitung von besonders sensiblen Daten, z. B. der Gesundheitsdaten, eine Kerntätigkeit der Praxis darstellt. Auch hier gehen die Aufsichtsbehörden aber mittlerweile davon aus, dass dies bei einer üblichen Praxis mit weniger als 10 Personen, die automatisiert personenbezogene Daten verarbeiten, nicht der Fall ist (siehe Entschließung der Datenschutzkonferenz unter https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/04/DSB-Bestellpflicht.pdf).

6. Schritt: Datensicherheit gewährleisten

In Art. 32 DSGVO wird zur Umsetzung der Datensicherheit darauf hingewiesen, dass der Verantwortliche geeignete technische und organisatorische Maßnahmen zu treffen hat, um ein dem Risiko angemessenes **Schutzniveau** zu gewährleisten. Dies soll „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“ geschehen. Die Vorschrift bleibt also sehr vage und gibt keine konkreten Anweisungen.

Was sagt uns das nun aber für unsere Praxis? Werden konkrete Maßnahmen vorgeschrieben? Es werden zwar in Art. 32 DSGVO die Verschlüsselung und Pseudonymisierung benannt, allerdings nur als Möglichkeiten, die nicht zwingend umzusetzen sind. Entscheidend ist, dass die für den jeweiligen Praxisinhaber machbaren Schritte zur Sicherung der Daten unternommen und auch dokumentiert werden.

Gerade in Anbetracht der Tatsache, dass es sich bei Patientendaten häufig um Gesundheitsdaten und damit datenschutzrechtlich besonders schützenswerte Daten handelt, werden aber hohe Anforderungen zu stellen sein. So ist durch eine **Zutritts- und Zugangskontrolle** zu gewährleisten, dass nur berechtigte Personen Zugang zu den Patientendateien haben. Ein Bereitlegen der Patientenkarteien für den nächsten Patienten in dem für die wartenden Patienten einsehbaren Rezeptionsbereich sollte daher dringend der Vergangenheit angehören! Zu empfehlen ist auch, dass die Karteien in einem verschlossenen Schrank aufbewahrt werden, zu dem nur berechtigte Personen den Schlüssel haben. Zudem ist der Computer mit einem Login-Passwort zu sichern, das nur an Berechtigte vergeben wird. Der Computer ist immer mit einer aktuellen Software zu bedienen und einem aktuellen Virenschutz zu versehen. Ein Backup-System sollte sicherstellen, dass selbst bei dem Übergriff durch Verschlüsselungstrojaner eine Verfügbarkeit der Daten weiterhin bestmöglich gewährleistet ist.

Sonderfall: Kommunikation via E-Mail oder Fax mit dem Patienten

Für viele Fragen sorgt die Kommunikation mit dem Patienten über E-Mail oder Fax. Es besteht zurzeit leider keine Einigkeit zwischen den Aufsichtsbehörden darüber, wie unter der Datenschutzgrundverordnung mit den Patienten kommuniziert werden darf. Klar ist, dass eine **Kommunikation** mit dem **Patienten** zur Umsetzung des Behandlungsvertrags erforderlich sein kann. Offen ist aber, ob hierunter auch eine Kommunikation per Fax oder E-Mail fällt. Denn weder Fax noch E-Mail sind ein gesicherter Kommunikationsweg, die Einsicht Dritter in die Kommunikationsinhalte ist nicht ausgeschlossen (Verschlüsselungstechniken ausgenommen). Es überwiegt die Ansicht, dass eine Kommunikation über Gesundheitsdaten wie Befundberichte, Diagnosen, Zwischenstände und Behandlungsverlauf über E-Mail oder Fax nur in „Notsituationen“, also ausnahmsweise, und daher nicht als Standardkommunikation zulässig ist.

Dieses Ergebnis scheint allerdings nicht praktikabel zu sein. Als **Lösungsansätze** gibt es zwei Alternativen:

1. Sie verzichten auf die genannten Kommunikationswege oder versenden im Falle der E-Mail-Kommunikation Gesundheitsdaten als verschlüsselten Anhang (z. B. ZIP-Verschlüsselung).
2. Sie holen die Einwilligung des Patienten zur Art der Kommunikation (per Fax oder per Email) für Terminabsprache und -koordination, aber auch für den sonstigen Austausch über den Gesundheitszustand ein. Dabei muss darauf hingewiesen werden, dass die Einwilligung für die Zukunft widerrufen werden kann. Zudem sollte auf die Unsicherheit der E-Mail- bzw. Fax-Kommunikation hingewiesen werden und auf die Tatsache, dass eine Einsicht von Dritten in die E-Mail- bzw. Fax-Inhalte nicht ausgeschlossen werden kann.

Abschreckende Sanktionen

Ein Verstoß gegen die EU-Datenschutzgrundverordnung kann die betroffene Praxis bis zu 20 Millionen Euro Geldbuße kosten – oder bis zu 4% dessen weltweiter Umsätze (je nachdem, welcher Wert am Ende höher ausfällt). Neu ist hierbei, dass die Verordnung ausdrücklich vorschreibt, dass die Sanktionen **„wirksam, verhältnismäßig und abschreckend“** sein sollen. Die Umsetzung der DSGVO ist daher unbedingt ernst zu nehmen.

Dieses Dokument wurde zum persönlichen Gebrauch heruntergeladen. Vervielfältigung nur mit Zustimmung des Verlages.

Zusammenfassung

Die DSGVO ist mit den beschriebenen Schritten umsetzbar und kann als Chance genutzt werden, in dem bei vielen Unternehmern und auch Praxisinhabern bestehenden Ansammlungen von Daten Transparenz und Ordnung zu schaffen. Die Umsetzung durch die Aufsichtsbehörden in den durch die DSGVO nicht in Details vorgegebenen Anforderungen lässt allerdings an Einheitlichkeit und Klarheit zu wünschen übrig. Von einer Einheitlichkeit der Rechtslage, die erklärtes Ziel der DSGVO war, kann daher schon in dem kleinen Land Deutschland nicht die Rede sein.

Autorinnen/Autoren

Sylke Wagner-Burkard
ist als Rechtsanwältin in eigener Praxis in der Rhön mit Schwerpunkt Recht der Heilberufe tätig. Als Justitiarin des Verbandes der Osteopathen Deutschland e.V. vertritt sie die rechtlichen Interessen des Verbands und berät die mehr als 4000 Mitglieder.

Korrespondenzadresse

Dr. iur. Sylke Wagner-Burkard, LL.M.
Neuwart 48
36163 Poppenhausen (Wasserkuppe)
info@kanzlei-wagnerburkard.de

Literatur

[1] Kühling J, Buchner B. Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DSGVO/BDSG, Kommentar. 2. Aufl. München: Beck; 2018

[2] Voigt P, von dem Bussche A. EU-Datenschutz-Grundverordnung, Praktikerhandbuch. Springer: Heidelberg; 2018

[3] Gierschmann S, Schlender K, Stentzel R, Veil W. Kommentar Datenschutz-Grundverordnung. Köln: Bundesanzeiger Verlag; 2018

Bibliografie

DOI https://doi.org/10.1055/a-0651-8540
DO – Deutsche Zeitschrift für Osteopathie 2018; 16: 1–7 © Georg Thieme Verlag KG Stuttgart · New York ISSN 1610-5044

Anzeige

Dieses Dokument wurde zum persönlichen Gebrauch heruntergeladen. Vervielfältigung nur mit Zustimmung des Verlages.