Rechtliche Hinweise und Formulierungshilfen zum Geltungsbeginn der europäischen Datenschutzgrundverordnung (DSGVO)

Ab dem 25. Mai 2018 gilt die DSGVO unmittelbar in allen Mitgliedsländern der Europäischen Union. In Deutschland löst die DSGVO das alte Bundesdatenschutzgesetz (BDSG) ab, welches die zuvor geltende Datenschutzrichtlinie 95/46/EG umsetzte. Ziel der Verordnung ist der Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Schutz bei der Verarbeitung personenbezogener Daten.

Der Deutsche Verband für Podologie (ZFD) e.V. hat nachfolgend die relevanten Änderungen, Rechte und Pflichten für die Inhaber einer Podologiepraxis zusammengestellt und mit Formulierungshilfen ergänzt:

Als Rechtsakt der Europäischen Union geht die DSGVO grundsätzlich allen nationalen Rechtsvorschriften vor, soweit nicht sogenannte Öffnungsklauseln in der DSGVO die Anwendung nationaler Regeln ausdrücklich erlauben. In Deutschland werden deshalb für den Schutz von Daten allgemein sowie der besonders sensiblen Gesundheitsdaten neben der DSGVO auch weiterhin das abgewandelte Bundesdatenschutzgesetz (BDSG neu), die zivilrechtlichen Vorschriften zum Behandlungsvertrag sowie das Sozialdatenschutzrecht gelten.

Auch unter dem Regime der DSGVO gilt für die Datenverarbeitung das sogenannte **Verbotsprinzip mit Erlaubnisvorbehalt**. Das bedeutet, dass alles verboten ist, es sei denn, es liegt eine ausdrückliche Erlaubnis vor. So dürfen Daten nur aufgrund gesetzlicher Erlaubnis oder aufgrund einer Einwilligung verarbeitet werden. Ansonsten ist ihre Erhebung, Weitergabe, Änderung etc. untersagt. Für die Verarbeitung von Gesundheitsdaten bietet Art. 9 Abs. 2 lit. h DSGVO einen umfassenden gesetzlichen Erlaubnistatbestand für die Arbeit in der podologischen Therapiepraxis, nämlich Datenverarbeitung zum Zweck der Versorgung oder Behandlung im Gesundheitsbereich sowie aufgrund eines Vertrags mit dem Angehörigen eines Gesundheitsberufs. Deshalb können Podologen auch in Zukunft ohne Einwilligungserklärung ihrer Patienten deren Gesundheitsdaten im Rahmen des Behandlungsvertrags verarbeiten.

1. Geheimhaltungspflicht

Wegen der besonderen Bedeutung von Gesundheitsdaten als besonders sensible Daten müssen alle Personen, die Gesundheitsdaten verarbeiten, einer Geheimhaltungspflicht unterliegen. Das ist bei Podologen und den Personen und Stellen, mit denen Podologen in Durchführung und Abwicklung des Behandlungsvertrags zusammenarbeiten, nämlich Ärzten, Angehörigen anderer Gesundheitsberufe, Krankenkassen, Abrechnungsstellen sowie weiteren Personen und Behörden, die dem Berufsgeheimnis unterliegen,

grundsätzlich der Fall (§ 203 StGB).
Besondere Aufbewahrungspflichten und Einsichtsrechte nach deutschem nationalen Recht (§§ 630 a ff. BGB - Behandlungsvertrag) bleiben aufgrund von Öffnungsklauseln der DSGVO weiterhin anwendbar.

2. **Einwilligung**
Für allgemeine Kontaktdaten, wie Name und Adresse gibt bereits der allgemeine Erlaubnistatbestand des Art. 6 Abs. 1 lit. b und f DSGVO (Vertrag, Interessenabwägung) eine ausreichende gesetzliche Grundlage. Nur in Ausnahmefällen, insbesondere bei Direktwerbung oder bei Veröffentlichung von Daten im Internet, sollte auch aus Gründen des Wettbewerbsrechts eine Einwilligung eingeholt werden.
(Formulierungshilfe DSGVO1)

3. **Informationspflichten**
Erhebliche Änderungen bringt die DSGVO dagegen für die formellen Pflichten des Verantwortlichen, d.h. der Person oder der Stelle, welche Daten verarbeitet. Dadurch sollen die zum Teil neuen und in ihrem Umfang erweiterten Datenrechtsgrundsätze, wie z.B. Transparenz, Integrität und Vertraulichkeit und Rechenschaft gewahrt werden. Deshalb müssen podologische Praxen umfassend über die von ihnen erhobenen Daten **informieren** und dabei gesetzliche Grundlagen, Verarbeitungszwecke, Empfänger und Betroffenenrechte angeben. Die Information erfolgt zum Zeitpunkt der Erhebung und wenn sich der Zweck der Datenverarbeitung ändert.
(Formulierungshilfe DSGVO2)

4. **Auskunftsrecht der betroffenen Person**
Andere formelle Pflichten folgen aus den Betroffenenrechten auf **Auskunft**, **Berichtigung**, **Löschung**, **Einschränkung der Verarbeitung**, **Datenübertragung** und **Widerspruch**. Die Auskunftserteilung ist dabei häufig die Grundlage für die Geltendmachung weiterer Rechte des Betroffenen und umfasst u.a. den Zweck der Verarbeitung, die Empfänger der Daten, die Dauer und einen Hinweis zum Recht auf Löschung oder Berichtigung unrichtiger Daten. Bei Auskunftsersuchen nicht gespeicherter Personen muss eine sogenannte Negativauskunft (dass keine Daten der Person verarbeitet wurden) erfolgen.
(Formulierungshilfe DSGVO3)

5. **Verzeichnis von Verarbeitungstätigkeiten**
   Zur Erfüllung ihrer Rechenschaftspflicht muss jede podologische Praxis ab dem 25. Mai 2018 ein sogenanntes Verzeichnis von Verarbeitungstätigkeiten führen (Art. 30 DSGVO). Der Ausnahmetatbestand des Art. 30 Abs. 5 DSGVO für Einrichtungen unter 250 Mitarbeitern ist wegen nicht nur gelegentlicher Datenverarbeitung bzw. Verarbeitung von Gesundheitsdaten nicht anwendbar. Das Verarbeitungsverzeichnis sollte sorgfältig geführt und regelmäßig aktualisiert werden. Es muss bei einer Überprüfung oder auf Anfrage der Aufsichtsbehörde vorgelegt werden.
   (Formulierungshilfe DSGVO4)

6. **Technische- und organisatorische Maßnahmen (T-O-M)**
   In das Verarbeitungsverzeichnis integriert oder gesondert hiervon sind Technische und Organisatorische Maßnahmen (T-O-M) aufzuführen, mit denen die Integrität und Vertraulichkeit der Datenverarbeitung gesichert werden sollen (Art. 24 DSGVO). Auch diese Pflicht entspringt der allgemeinen Rechenschaftspflicht des datenverarbeitenden Verantwortlichen, der nach dem sog. risikobasierten Ansatz der DSGVO aufgrund seiner eigenen Risikoeinschätzung entscheiden muss, welche Sicherungsmaßnahmen zu ergreifen sind. Dazu gehört nicht nur die Verpflichtung von Mitarbeitern zur Verschwiegenheit, sondern auch die geschützte Aufbewahrung der Patientendaten und die Sicherung vor Verlust und Beschädigung.
   (Entscheidungshilfe DSGVO7)

7. **Datenschutz-Folgeabschätzung (DSFA)**
   Eine Datenschutz-Folgeabschätzung (DSFA) - ebenfalls als Ausdruck der Rechenschaftspflicht - muss eine podologische Praxis dagegen nur dann vornehmen, wenn sie Gesundheitsdaten in großem Umfang verarbeitet (Art. 35 Abs. 3 lit. b DSGVO). Aus Erwägungsgrund 91 zur DSGVO geht hervor, dass die Verarbeitung von Gesundheitsdaten durch einen **einzelnen** Angehörigen eines Gesundheitsberufs nicht als umfangreich angesehen wird. Eine klare Mengenangabe zur „umfangreichen" Verarbeitung lässt die DSGVO offen und so ist abzuwarten, wann die Aufsichtsbehörden sogenannte Positiv- und ggf. Negativlisten gemäß Art. 35 Abs. 4 und 5 DSGVO aufstellen, in welchen die Notwendigkeit einer Datenschutz-Folgeabschätzung für einzelne Verarbeitungsvorgänge rechtssicher festgestellt wird.

8. **Der Datenschutzbeauftragte (DSB)**
   Die Benennung eines Datenschutzbeauftragten in einer podologischen Praxis ist gemäß § 38 Abs. 1 Satz 1 BDSG (neu) nur erforderlich, wenn in der Regel mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.

Als automatisierte Verarbeitung gelten z.B. die Nutzung von Papier- oder digitalen Kundendateien, die Verwendung von Kundendaten auf einem Tablet-PC oder einem Smartphone. Für die Zählung der Angestellten ist nicht die Arbeitszeit, sondern die Kopfanzahl der regelmäßig Beschäftigten maßgeblich. Als Datenschutzbeauftragter kann sowohl ein Mitarbeiter der Praxis als auch ein externer Dienstleister benannt werden. Er muss in seiner Aufgabenwahrnehmung als DSB weisungsfrei sein und sowohl über IT-Fachwissen als auch über Datenschutzrechtskenntnisse verfügen. Der Praxisinhaber selbst kann sich nicht selbst als DSB benennen, da er sonst in einen Interessenskonflikt gerät. Soll ein Mitarbeiter als Datenschutzbeauftragter benannt werden, bietet sich eine qualifizierte Schulung mit Prüfung und Zertifikat bei einem seriösen Anbieter, bspw. TÜV, an. Die Kontaktdaten des Datenschutzbeauftragten sind in der datenschutzrechtlichen Information ebenfalls zu nennen.
(Formulierungshilfe DSGVO5)

9. Auftragsverarbeitung

Von erheblicher Praxisrelevanz ist die Auftragsverarbeitung, bei der Dritte vom Praxisinhaber mit der Datenverarbeitung betraut werden. Durch die DSGVO wurden dabei die datenschutzrechtlichen Verantwortlichkeiten des Auftragsverarbeiters mit denen des Verantwortlichen weitgehend gleichgestellt (Art. 28 Abs. 3 DSGVO). Der Verantwortliche darf nur Auftragsverarbeiter auswählen und beauftragen, die die Rechtmäßigkeit der Datenverarbeitung garantieren. Obwohl Art. 28 DSGVO keine besondere Form für die Auftragsverarbeitung vorsieht, ist es in der Praxis aus Beweisgründen empfehlenswert, einen Vertrag in Textform zu schließen.
(Formulierungshilfe DSGVO7)

Die DSGVO ist relativ technikneutral gefasst. Sie enthält keine Definitionen und konkreten Zulässigkeitstatbestände für technische Sachverhalte wie Big Data, Cloud Computing, eHealth etc. Auch die Videoüberwachung wird von der DSGVO explizit nicht geregelt. Es sind insoweit das Überwachungsinteresse des Praxisinhabers (Durchsetzung des Hausrechts, Prävention und Aufklärung von Straftaten) und das allgemeine Persönlichkeitsrecht der überwachten Personen gemäß Art. 6 Abs. 1 lit. f DSGVO gegeneinander abzuwägen. Daraus folgt, dass in der Regel nur der Eingangs- und Kassenbereich einer Praxis überwacht werden darf, keinesfalls die Behandlungsräume, und dass auf die Videoüberwachung hingewiesen werden muss. Dies sollte in Form eines Hinweisschildes mit Name und Kontaktdaten der verantwortlichen Person am Eingang der Praxis erfolgen (§ 4 Abs. 2 BDSG nF).

Die DSGVO regelt nicht den Datenschutz bei **elektronischer Kommunikation** (Art. 95 DSGVO). Insoweit soll in Zukunft die sogenannte E-Privacy-Verordnung zur Anwendung kommen, die aber voraussichtlich erst im Jahr 2019 in Kraft treten und gelten wird. Bis dahin dürfte die bestehende Regelungslücke durch Anwendung der DSGVO zusammen mit den Bestimmungen des Telemediengesetzes in Umsetzung der Richtlinie über den Datenschutz bei elektronischer Kommunikation (RL 2002/58/EG) gefüllt werden. Bei Betreiben einer Webseite sollten deshalb vorsorglich zu den bisherigen Datenschutzhinweisen nach dem Telemediengesetz weitere Hinweise gemäß den Bestimmungen der DSGVO hinzugefügt werden (Formulierungshilfe 8)

Begriffsbestimmung (Art. 4 DSGVO):

personenbezogene Daten: alle Informationen, die sich auf eine natürliche Person (= betroffene Person) beziehen und anhand der Daten eine eindeutige Zuordnung und Identifizierung der natürlichen Person erfolgen kann
Gesundheitsdaten: alle personenbezogenen Daten einer natürlichen Person, die sich auf die körperliche oder geistige Gesundheit einschließlich der Gesundheitsdienstleistungen beziehen und aus denen der Gesundheitszustand hervorgeht
Verarbeitung: jeder - mit oder ohne Hilfe automatisierter Verfahren - ausgeführter Vorgang zur Erhebung, Erfassung, Organisation, Ordnung, Speicherung, Anpassung, Veränderung, Verwendung, Übermittlung, Löschung oder Vernichtung
Dateisystem: jede nach bestimmten Kriterien strukturierte Datensammlung (z.B. Patientenkartei in digitaler **und** Papierform)
Verantwortlicher: jede natürliche oder juristische Person, Einrichtung, Behörde oder andere Stelle, die über den Zweck und die Mittel der Datenverarbeitung entscheidet (z.B. Praxisinhaber, Datenschutzbeauftragter)
Auftragsverarbeiter: eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (z.B. Mitarbeiter, Abrechnungszentrum)
Einwilligung: für einen bestimmten Fall von der betroffenen Person unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder sonstigen eindeutigen Handlung, mit der die betroffene Person ihr Einverständnis zur Verarbeitung der personenbezogenen Daten gibt

Weitere Informationen:
Link DSGVO
Link BDSG (neu)

Stand: April 2018