LawConcepts®

Gutachten:

Datenschutzrechtliche Belehrung durch den ärztlichen Behandler beim Einsatz von rtCGM-Systemen in der diabetologischen Praxis

RA Dr. Arnd-Christian Kulow
DSB/DSA/QMB (TÜV SÜD)

Stand: Juli 2020

Inhaltsverzeichnis

A. Sachverhalt

Bei einer Diabeteserkrankung ist es wichtig, einen möglichst lückenlosen Verlauf bestimmter Stoffwechseldaten zu haben. Hierzu gibt es Anbieter (vgl. Anlage 2), die mittels Sensoren diese Stoffwechseldaten beim Patienten erheben und in einer Cloud (im Folgenden: CGM-Cloud) speichern. Den Vertrag mit dem CGM-Cloud-Anbieter schließt der Patient. Der behandelnde Arzt oder die behandelnde Ärztin stellen die Eignung des Patienten für die CGM-Cloud fest und empfehlen den Einsatz der CGM-Cloud.

Der Patient hat regelmäßig die Möglichkeit Dritten, also auch dem behandelnden Arzt oder der behandelnden Ärztin, den Zugang zu diesen Daten zu ermöglichen. Hierzu muss der Patient eine entsprechende Erklärung gegenüber dem Anbieter der CGM-Cloud abgeben. Für die Behandler stellen die CGM-Cloud-Anbieter regelmäßig einen besonderen Zugang zur Verfügung. Liegt vom Patienten eine entsprechende Erklärung vor, kann der Behandler über seinen eigenen Praxiszugang auf die Daten des Patienten zugreifen.

Es entsteht bezüglich der Verarbeitung der Stoffwechseldaten des Patienten ein Dreiecksverhältnis zwischen Patient, Arzt und CGM-Cloud-Anbieter.

B. Aufgabenstellung

Unter Anlage 1 findet sich der Vorschlag für eine entsprechende Datenschutzerklärung. Diese soll von den Praxen dem Patienten vorgelegt werden und von diesem unterschrieben werden.

Der oben dargestellte Sachverhalt und insbesondere die Datenschutzerklärung gemäß Anlage 1 ist datenschutzrechtlich zu würdigen. Prüfungsmaßstab ist daher das europäische und nationale Datenschutzrecht. Ferner ist das ärztliche Berufsrecht zu beachten, da auch dieses die Persönlichkeitsrechte des Patienten zu schützen hat.

C. Kurzstellungnahme

1) Die CGM-Cloud-Anbieter benötigen von den Patienten eine wirksame Einwilligung.

Nach grober, exemplarischer Prüfung von zwei entsprechenden Erklärungen bestehen Zweifel, ob dies tatsächlich erreicht wird. Die Erklärungen sind zu umfangreich und nicht gut aufbereitet. Sie könnten daher für den Patienten intransparent sein. Zudem dürfte die persönliche Drucksituation des Patienten das notwendige Vorliegen von „Freiwilligkeit“ stark erschweren.

2) Die behandelnden Ärztinnen und Ärzte benötigen – anders als in dem vorliegenden Erklärungsmuster vorgesehen – keine besondere Einwilligung für den Zugriff und die Verarbeitung der Messwerte in der Cloud.

3) Dieses Ergebnis ist unbefriedigend, weil der Patient allein gelassen wird.

Er ist in der Regel nicht in der Lage, die korrekte Verwendung der Daten in der CGM-Cloud zu kontrollieren. Auch für die Praxen ist das Ergebnis berufsrechtlich unbefriedigend, da diese zwar die CGM-Cloud empfehlen, einen entsprechenden Datenschutz aber ebenfalls nicht versprechen können. Das spiegelt der Hinweis auf die "Verarbeitung in den USA" in dem vorliegenden Muster. Leider ist es mit so einem Hinweis nicht getan, der Patient kann ja damit kaum was anfangen. Man sieht aber das Bemühen der Praxis, sich irgendwie "freizuzeichnen".

4) Es handelt sich bei dem zu begutachtenden Sachverhalt um ein zweckgebundenes Dreiecksverhältnis der Gesundheits-Datenverarbeitung.

Bei diesem ist der Patient als Betroffener außerordentlich schutzwürdig im Sinne der DSGVO und des ärztlichen Berufsrechts. Gleichwohl ist eine weitergehende datenschutzbezogene Aufklärungs- oder gar Kontrollpflicht derzeit berufsrechtlich nicht zu fordern.

5) Für Dreiecksverhältnisse mit gemeinsamen Zwecken und Mitteln geht die DSGVO regelmäßig vom Vorliegen einer gemeinsamen Verantwortlichkeit nach Art. 26 DSGVO aus.

So liegt es auch bei dem zu prüfenden Sachverhalt. Arzt und CGM-Cloud-Anbieter sind dem Patienten gegenüber gemeinsam nach Art. 26 DSGVO verantwortlich, weil sie beide die CGM-Cloud als Mittel und zum Zweck der Behandlung des Diabetes des Patienten einsetzen. Sie müssen daher zwingend einen entsprechenden Vertrag schließen, der die Zuständigkeiten gegeneinander abgrenzt. Der Patient ist entsprechend zu informieren.

6) Die Verwendung der Musterklärung gemäß Anlage 1 wird nicht empfohlen. Die DDG sollte vielmehr mit den Beteiligten eine Mustervereinbarung nach Art. 26 Abs. 1 Satz 2 DSGVO erarbeiten.

D. Gutachten

I. Rechtmäßigkeit der Erhebung und Speicherung der Stoffwechseldaten durch die CGM-Cloud-Anbieter

1) Durch Vertrag nach Art. 6 Abs. 1 lit. b) DSGVO

Als Rechtmäßigkeitsbedingung („Erlaubnistatbestand“) der Erhebung und Speicherung der Messwerte und Adressdaten des Patienten kommt hier zunächst ein Vertrag iSd. zwischen dem CGM-Cloud-Anbieter und dem Patienten in Betracht. Vom Vorliegen einer solchen vertraglichen Beziehung mit den Patienten ist bei den Anbietern in Anlage 2 regelmäßig auszugehen. Nach Art. 4 Ziffer 15 DSGVO handelt es sich jedoch bei den erhobenen Messdaten um Gesundheitsdaten iSd. der DSGVO, weil es sich bei den Messwerten um personenbezogene Daten handelt, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.

Die Verarbeitung solcher Daten ist nach Art. 9 Abs. 1 DSGVO generell untersagt. Ausnahmen finden sich nur in Art. 9 Abs. 2 DSGVO.

2) Nach Art. 9 Abs. lit. h) DSGVO, „Behandlungsvertrag“

Hier käme unter Umständen die Ausnahmeregelung des Art. 9 Abs. lit. h) DSGVO in Betracht. Demnach wäre eine Verarbeitung für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs möglich.

Es ist fraglich, ob das Speichern der Stoffwechseldaten in der Cloud einer der genannten Fallgruppen des Art. 9 Abs. lit. h) DSGVO unterfällt. Vom Wortlaut her kämen zumindest die Verarbeitung zu Zwecken der medizinischen Diagnostik, der Versorgung bzw. Behandlung im Gesundheitswesen in Betracht. Allerdings müssen diese Ausnahmezwecke in jedem Fall eng ausgelegt werden[1]. Zudem dient die Norm dem individuellen Interesse des Betroffenen an der gesundheitlichen Versorgung[2]. Dies könnte zwar unter Umständen hier zugunsten der CGM-Cloud-Anbieter noch angenommen werden, allerdings fordert Art. 9 Abs. 3 DSGVO stets die Verarbeitung durch Fachpersonal, das dem Berufsgeheimnis unterliegt. Verarbeiten andere Personen, also nicht ärztliches Fachpersonal, so müssen diese nach nationalen oder unionsrechtlichen Vorschriften jedenfalls einer entsprechenden Geheimhaltungspflicht unterliegen. Hiervon kann bei den CGM-Cloud-Anbietern wohl nicht ausgegangen werden. So auch ausdrücklich Sassenberg/Faber:

> „Bei der Verwendung von digitalen Gesundheitsprodukten — etwa wie in obiger *Abbildung 1* Sensor, App und Injektionspen oder in obiger *Abbildung 2* Sensor, Steuerungseinheit, Bluetooth Transmitter und Wirkstoff-Depot — muss ausreichend für den Schutz der sensiblen Gesundheitsdaten gesorgt sein. Mit diesen Geräten erhebt und verarbeitet gerade nicht ärztliches Personal die Gesundheitsdaten des Patienten — wie im Bereich der klinischen Prüfung, sondern der Patient selbst. Damit scheidet auch der Erlaubnistatbestand nach § 28 Abs. 7 BDSG (Gesundheitsvorsorge) aus. Es kommt für die Zulässigkeit der Datenverarbeitung auf die Einwilligung des Patienten an.“[3]

Zwischenergebnis: Da jedenfalls eine Verarbeitung durch dem Berufsgeheimnis bzw. einer ähnlichen Geheimhaltungspflicht unterliegendes Personal nicht stattfindet, ist hier nicht von einer einwilligungsfreien Verarbeitung nach Art. 9 Abs. 2 lit. h DSGVO auszugehen.

3) Nach Art. 9 Abs. 2 lit. a) DSGVO, „Einwilligung“

1 Kühling/Buchner, DS-GVO Kommentar, 2. Aufl, 2018, Rz. 46 zu Art. 9.
2 Kühling/Buchner, DS-GVO Kommentar, 2. Aufl, 2018, Rz. 93 zu Art. 9.
3 Sassenberg/Faber, Rechtshandbuch Industrie 4.0 und Internet of Things, 2. Aufl., 2020, Rn. 89.

Es kommt daher vielmehr auf eine wirksame Einwiligung nach Art. 9 Abs. 2 lit. a) DSGVO an. Dies insbesondere deshalb, weil dem Betroffenen vom CGM-Cloud-Anbieter hier regelmäßig eine App zur Verfügung gestellt wird.[4]

Die Rechtmäßigkeit der Erhebung und Verarbeitung der Messwerte durch den CGM-Cloud-Anbieter hängt daher von dem Vorliegen einer wirksamen Einwilligung ab.

Die Überprüfung des Vorliegens einer jeweils wirksamen Einwilligung bei den diversen Anbietern ist nicht Gegenstand dieses Gutachtens.

Ergebnis: Die datenschutzrechtliche Rechtmäßigkeit der Verarbeitung der Messdaten der Betroffenen hängt von einer wirksamen Einwilligung des Betroffenen ab.

II. Rechtmäßigkeit der Datenverarbeitung durch die Arztpraxis

1) Verarbeitung aufgrund des Behandlungsvertrags nach §§ 630a ff. BGB

Als Rechtsgrundlage der Verarbeitung kommt der Behandlungsvertrag nach §§ 630a ff. BGB in Betracht. Dieser bietet regelmäßig die Rechtsgrundlage zur Verarbeitung von personenbezogenen Daten des Patienten durch ärztliche Behandler. Nach Art. 9 Abs. 2 lit. h) DSGVO, § 22 Abs. 1 1.b) BDSG gilt das auch für die Gesundheitsdaten. Hier liegt eine medizinische Behandlung vor, diese umfasst die individuelle Betreuung einer Diabeteserkrankung des Betroffenen. Der Begriff schließt Diagnostik und Therapie mit ein. Dazu gehört auch die Verwendung von in der Cloud vom Patienten gespeicherten Daten zur besseren Behandlung der Diabeteserkrankung.

Im Übrigen ist die Gewährleistung der Verarbeitung durch Fachpersonal, das dem Berufsgeheimnis unterliegt, nach Art. 9 Abs. 3, 1. Alt. DSGVO, § 22 Abs. 1 1.b) BDSG gegeben.

4 Sassenberg/Faber, Rechtshandbuch Industrie 4.0 und Internet of Things, 2. Aufl., 2020, Rn. 90.

Zwischenergebnis: Die Arztpraxis kann auch die Verarbeitung der Daten aus der CGM-Cloud auf den mit dem Betroffenen geschlossenen Behandlungsvertrag nach §§ 630a ff. BGB stützen.

2) Zusätzliche Einholung einer Einwilligung nach Art. 9 Abs. 2 lit. a) DSGVO, § 630d Abs. 1 BGB, laut Mustertext (Anlage 1)

Im Mustertext (Anlage 1) lautet der dritte und letzte Absatz folgendermaßen:

> „Ich bin mit der Nutzung der Online-Software durch die Praxis einverstanden. Meine Einwilligung kann ich in der Praxis jederzeit widerrufen. In dem Fall würden meine Daten im System des Hersteller wieder gelöscht werden."

a) Überlagerungswirkung der Einwilligung auf andere Erlaubnistatbestände

Die hier im Mustertext (nach Anlage 1) vorgesehene Einholung einer Einwilligung des Patienten zur Nutzung der in der CGM-Cloud gespeicherten Daten ist grundsätzlich möglich. Die DSGVO geht davon aus, dass mehrere Rechtmäßigkeitsbedingungen vorliegen können. So wäre es hier durchaus möglich, zusätzlich zum an sich ausreichenden Behandlungsvertrag „zur Sicherheit" noch eine Einwilligung einzuholen. Dies hat aber schwerwiegende Nachteile. Bestehen neben der Einwilligung noch gesetzliche Rechtmäßigkeitsbedingungen, wie hier der Behandlungsvertrag, so darf sich der ärztliche Behandler bei einem Widerruf der Einwilligung durch den betroffenen Patienten nicht mehr auf den Behandlungsvertrag berufen:

> „Holt die datenverarbeitende Stelle bei der betroffenen Person eine Einwilligung ein, signalisiert sie ihr, dass es für die Zulässigkeit einer Datenverarbeitung allein auf ihr Einverständnis ankommen soll. Dann wäre es aber in sich widersprüchlich und damit unzulässig, wenn die datenverarbeitende Stelle im Falle der Verweigerung oder Unwirksamkeit einer

> Einwilligung alternativ doch wieder auf einen gesetzlichen Erlaubnistatbestand zurückgreifen könnte.“[5]

Damit könnte der ärztliche Behandler im Falle des Widerrufs der Einwilligung die Gesundheitsdaten auch nicht mehr nach § 630a ff. BGB verarbeiten. Gleichwohl bliebe die berufsrechtliche Verpflichtung zur medizinisch wirksamen Behandlung bestehen. Ohne die entsprechenden Messwerte des Patienten ist das nur schwer vorstellbar.

b) Wirksamkeit der Einwilligung nach Art. 7 DSGVO

Die vorliegende Mustereinwilligung genügt zudem nicht den Anforderungen an eine wirksame Einwilligung für diesen Sachverhalt.

Diese muss nicht nur ein „erhöhtes Maß an Bestimmtheit und Genauigkeit“[6] haben und sich ausdrücklich auf Gesundheitsdaten beziehen, sondern auch freiwillig und in voller Kenntnis der wesentlichen Umstände der beabsichtigten Verarbeitung erteilt werden.

Schon am Bestehen der Freiwilligkeit bestehen hier Bedenken. Besteht nämlich ein Abhängigkeitsverhältnis zwischen dem Verantwortlichen und dem Betroffenen — wie hier zwischen Arzt und Patient –, so sind besonders hohe Anforderungen an die Freiwilligkeit der Einwilligung zu stellen.[7] Zwar kann man nicht generell von einer Unwirksamkeit der Einwilligung in diesen Fällen ausgehen[8], gleichwohl befindet sich der Patient hier in einer Situation, in der er keine wirkliche Alternative hat. Verweigert er nämlich die Einwilligung, so scheidet für ihn die Möglichkeit die CGM-Cloud zu nutzen, aus. Jedenfalls wenn der Behandler auf einer Einwilligung besteht. Hier müssten also dem Patienten sehr deutlich die Chancen und Risiken einer Datenspeicherung in der CGM-Cloud vor Augen geführt werden. Das ist augenscheinlich bei dem Mustertext nicht der Fall. Im Gegenteil: In dem der dritte Absatz des Mustertextes verspricht, dass im Falle des Widerrufs die Daten in der CGM-Cloud gelöscht würden, belehrt er unrichtig. Der Widerruf der Einwilligung der Verarbeitung durch den ärztlichen Behandler berührt ja das Verhältnis Patient-CGM-Anbieter nicht. Der Widerruf hätte nur zur Folge, dass der ärztliche Behandler nicht mehr auf die Daten zugreifen darf. Diese blieben aber auf dem Server des CGM-Cloud-Anbieters weiter gespeichert.

---

5 Kühling/Buchner, DS-GVO Kommentar, 2. Aufl., 2018 , Rz. 23 zu Art. 6.
6 Kühling/Buchner, DS-GVO Kommentar, 2. Aufl., 2018 , Rz. 47 zu Art. 9.
7 Kühling/Buchner, DS-GVO Kommentar, 2. Aufl., 2018 , Rz. 51 zu Art. 9.
8 Kühling/Buchner, DS-GVO Kommentar, 2. Aufl., 2018 , Rz. 51 zu Art. 9.

Nach dem ist von der zusätzlichen Einholung einer Einwilligung nach Art. 9 Abs. lit.a) DSGVO dringend abzuraten. Die Anforderungen sind hoch und im Widerrufsfall ist der ärztliche Behandler unter Umständen nicht mehr in der Lage, den Behandlungsvertrag zu erfüllen.

Zwischenergebnis:

Es besteht keine datenschutzrechtliche Verpflichtung der ärztlichen Behandler, für den Zugriff auf die Messwerte des Patienten in der CGM-Cloud, eine Einwilligung des Patienten einzuholen.

III. Berufsrechtliche Pflicht zur datenschutzrechtlichen Beratung des Patienten?

Datenschutzrechtliche Informations- und Aufklärungspflicht aus §§ 630c Abs. 2, 630e Abs. 1 BGB

Das oben erhaltene Zwischenergebnis ist datenschutzrechtlich nicht befriedigend. Der speziellen Situation des Patienten wird nicht ausreichend Rechnung getragen. Dieser ist nämlich der schwächste Part in der Dreieckskonstellation. Ihm geht es verständlicherweise in erster Linie um die Behandlung seines Diabetes. Das wirft die Frage nach einem adäquaten Patientenschutz in diesen Konstellationen auf. Daher fragt sich insbesonders, inwieweit sich eine datenschutzrechtliche Beratungspflicht der ärztlichen Behandler aus dem Berufsrecht ableiten lässt.

Hierbei ist zu klären, ob und in welchem Umfang auch eine datenschutzrechtliche Informations- und Aufklärungspflicht von den §§ 630c Abs. 2 und 630e Abs. 1 BGB umfasst ist.

Nach § 630c Abs. 2 BGB ist der Behandelnde verpflichtet, dem Patienten in verständlicher Weise zu Beginn der Behandlung und, soweit erforderlich, in deren Verlauf sämtliche für die Behandlung wesentlichen Umstände zu erläutern, insbesondere die Diagnose, die voraussichtliche gesundheitliche Entwicklung, die Therapie und die zu und nach der Therapie zu ergreifenden Maßnahmen.

Zu erörtern ist also, ob die datenschutzrechtliche Lage zu den wesentlichen Umständen der Behandlung zählt. Bei der großen Bedeutung der Gesundheitsdaten eines Menschen für das allgemeine Persönlichkeitsrecht und das Selbstbestimmungsrecht könnte es schon zu den Hauptleistungspflichten aus dem Behandlungsvertrag gehören, den Patienten — gerade bei Inanspruchnahme von weiteren Datenverarbeitern, wie hier — über die datenschutzrechtlichen Implikationen aufzuklären.

Vom Gesetzeswortlaut her bezieht sich die Informations- und Aufklärungspflicht auf „die Behandlung“. Der Begriff der medizinischen Behandlung ist nicht legal definiert. Er umfasst nach allgemeiner Meinung, neben der Diagnose, alle Heileingriffe und therapeutischen Maßnahmen an Körper oder Geist eines Menschen.[9] Der Behandlungsbegriff ist daher körperbezogen. Er würde derzeit wohl überdehnt, wollte man auch die Sorge um das Persönlichkeitsrecht des Patienten mit zu den wesentlichen Umständen des Heileingriffs zählen. Für diese Auslegung spricht auch, dass der Gesetzgeber de lege lata die Aufklärung zu wirtschaftlichen Fragen separat im § 630c Abs. 3 BGB geregelt hat. Diese werden ebenfalls nicht vom Begriff der medizinischen Behandlung umfasst und wurden daher in einem speziellen Absatz geregelt.

Im Übrigen würde eine Aufklärung über die generellen Risiken der Verarbeitung bei Dritten, wie hier bei den CGM-Cloud-Anbietern dem Patienten nicht viel bringen. Der ärztliche Behandler kann, da er ja die Server nicht kontrolliert, kaum relevante Aussagen zur Datenschutzlage bei den CGM-Anbietern machen.

Ergebnis:

Eine umfassende datenschutzrechtliche Aufklärung durch die ärztlichen Behandler ist berufsrechtlich nicht geboten.

IV. Gemeinsame Verantwortlichkeit gem. Art. 26 DSGVO

1) Voraussetzungen des Art. 26 DSGVO

9 So in etwa: Palandt/Weidenkaff, 75. Aufl., 2016, Rz. 2 Vorb v 630a: „Maßnahmen an Körper oder Gesundheit [sic!] eines Menschen“

Nach Art. 26 sind zwei oder mehrere Verantwortliche als gemeinsam verantwortlich anzusehen, wenn sie gemeinsam die Zwecke der und die Mittel zur Verarbeitung festlegen. Sie müssen in diesem Fall in einer Vereinbarung in transparenter Form festhalten, wer von ihnen welche Verpflichtung gemäß der DSGVO erfüllt, insbesondere, was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 nachkommt, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festgelegt sind. In der Vereinbarung kann eine Anlaufstelle für die betroffenen Personen angegeben werden.

Der Tatbestand des Art. 26 besteht nach Abs. 1 Satz 1 1. HS. im gemeinsamen Festlegen der Mittel und Zwecke der Verarbeitung. Dies ist allerdings nicht so zu verstehen, dass die Annahme einer gemeinsamen Verantwortung nur dann in Betracht kommt, wenn es zu einer gemeinsamen Festlegung der Zwecke und Mittel zwischen den Beteiligten bereits gekommen ist. Es ist vielmehr gestuft zu prüfen, ob zwei selbstständig Verantwortliche gegeben sind und in einem zweiten Schritt, ob diese funktional und tatsächlich gemeinsam die Zwecke und Mittel bestimmen.[10] Es kommt daher für die Annahme einer gemeinsamen Verantwortung nicht notwendigerweise auf die Einschätzung der Beteiligten an, sondern auf die tatsächlichen Umstände des Zusammenwirkens.[11]

a) Mehrere datenschutzrechtlich eigenverantwortlich handelnde Akteure

Wer die Zwecke und die Mittel einer Verarbeitung von personenbezogenen Daten festlegt, ist nach der DSGVO stets als Verantwortlicher anzusehen (Art. 4 Ziffer 7 DSGVO).

Unproblematisch sind sowohl die CGM-Cloud-Anbieter als auch die ärztlichen Behandler als selbstständige Verantwortliche anzusehen, denn sie entscheiden in Bezug auf den Patienten autonom über den Zweck der Datenverarbeitung und die dazu eingesetzten Mittel.

Es ist daher insbesondere kein Raum für die Annahme einer Auftragsverarbeitung gemäß Art. 28 DSGVO etwa zwischen ärztlichen Behandlern und CGM-Cloud-Anbietern.

10 Kühling/Buchner, DS-GVO Kommentar, 2. Aufl., 2018, Rz. 14 zu Art. 26; Gierschmann/Schlender/Stentzel/Veil, DSGVO, 2018, Rz. 33 zu Art. 26.
11 Gierschmann/Schlender/Stentzel/Veil, DSGVO, 2018, Rz. 33 zu Art. 26.

b) Gemeinsame Zwecke und Mittel?

Zu prüfen ist nunmehr, ob hier gemeinsame Zwecke mit einem gemeinsamen Mittel verfolgt werden.

Die Formen der gemeinsamen Verantwortung nach Art. 26 DSGVO können sehr vielfältig sein.[12]

> „Sie kann sehr eng sein in Form vollständig übereinstimmender Mittel und Zwecke oder aber nur locker bzw. teilweise, indem die einzelnen Parteien nur für Zwecke, nur für Mittel oder nur Teile davon verantwortlich zeichnen.“[13]

Für eine Annahme des Art. 26 DSGVO muss die Verarbeitung der Daten auch nicht gleichzeitig stattfinden. Die Daten können vielmehr auch nacheinander verarbeitet werden.[14]

Bei der vorliegenden Fallgestaltung ist der gemeinsame Zweck, die verbesserte Behandlung von Diabeteserkrankungen. Hierbei wirken der CGM-Cloud-Anbieter und der ärztliche Behandler eng zweckgebunden zusammen. Zwar kann der Zugang zu den Messdaten vom Betroffenen auch nicht ärztlichen Personen gewährt werden, nach Sinn und Zielsetzung gerade der Cloudspeicherung stehen jedoch die ärztlichen Behandler im Mittelpunkt. Zudem sind sie es auch, die festzustellen haben, ob die Cloudspeicherung der Messdaten für die Behandlung sinnvoll ist. Vom Vorliegen eines gemeinsam gegenüber dem betroffenen Patienten verfolgten Zwecks ist daher auszugehen.

Es fragt sich, ob die Cloudspeicherung der Daten auch ein gemeinsames Mittel im Sinne des Art. 26 Abs. 1 DSGVO ist. Hier könnte man einwenden, dass insbesondere die ärztlichen Behandler mit der Cloudspeicherung nichts zu tun haben. Ähnlich wie beim Verschreiben eines Medikaments, gebe es zwar einen gemeinsamen Zweck mit dem Medikamentenhersteller, jedoch keine gemeinsamen Mittel.

Die Frage, ob hier eine gemeinsame Verantwortung anzunehmen ist, beantwortet sich allerdings gerade nicht aus der Sicht der beteiligten Verantwortlichen, sondern aus der Perspektive der betroffenen Patienten.[15]

Diesen gegenüber verwenden beide Verantwortliche das Mittel der Zugänglichmachung der Daten in der Cloud. Den Arztpraxen wird hier regelmäßig eine auf Arztpraxen zugeschnittene Zugangsmöglichkeit eingeräumt. Sowohl CGM-Cloud-Anbieter, als auch Ärzte und Ärztinnen nutzen die Clouddaten

12 Sydow (Hrsg.), DSGVO, 2018, Rz. 4 zu Art. 26: „potentiell alle Formen kumulativen Zusammenwirkens“.
13 Kühling/Buchner, DS-GVO Kommentar, 2. Aufl., 2018, Rz. 15 zu Art. 26 m.w.N.
14 Kühling/Buchner, DS-GVO Kommentar, 2. Aufl., 2018, Rz. 16 zu Art. 26 m.w.N.
15 Gierschmann/Schlender/Stentzel/Veil, DSGVO, 2018, Rz. 11 zu Art. 26.

geschäftsmäßig gemeinsam, dieses Vorgehen stellt für sie damit ein gemeinsames Mittel dar, mit dem beide Teile ihres Einkommens erzielen.[16]

Es ist daher davon auszugehen, dass ärztliche Behandler und CGM-Cloud-Anbieter zur Erreichung des gemeinsamen Zwecks der Verbesserung der Behandlung einer Diabeteserkrankung der Betroffenen das gemeinsame Mittel der Datenspeicherung in der Cloud einsetzen.[17]

Damit sind sie als gemeinsam verantwortlich iSd. Art. 26 DSGVO anzusehen.

Zwischenergebnis:

Ärztliche Behandler mit Zugang zu einer CGM-Cloud sind gemeinsam mit dem Anbieter der Cloud für die Daten der Patienten nach Art. 26 DSGVO verantwortlich.

Dieses Ergebnis entspricht auch dem Sinn und Zweck des Instituts der gemeinsamen Verantwortung. Schon vor Geltung der DSGVO hat sich die die Art.-29-Datenschutzgruppe in einem grundlegenden Papier aus dem Jahr 2010 ganz grundsätzliche Gedanken zur gemeinsamen Verantwortung in komplexen Verarbeitungssachverhalten gemacht:

> „The bottom line should be ensuring that even in complex data processing environments, where different controllers play a role in processing personal data, compliance with data protection rules and responsibilities for possible breach of these rules are clearly allocated, in order to avoid that the protection of personal data is reduced or that a "negative conflict of competence" and loopholes arise whereby some obligations or rights stemming from the Directive are not ensured by any of the parties. In these cases, more than ever, it is important that a clear information notice is given to the data subjects, explaining the various stages and actors of the processing. Moreover, it should be made clear if every controller is competent to comply with all data subject's rights or which controller is competent for which right.
>
> [...]
>
> In this perspective, the assessment of joint control should take into account on the one hand the necessity to ensure full compliance with data protection

16 Vgl. Martini in: Paal/Pauly, DSGVO/BDSG, 2. Aufl., 2018, Rz. 21 zu Art. 26: „kooperative Determinierung des Zielzustandes, […] und der Mittel, die bei dessen Erreichung zum Einsatz kommen“.

17 Gierschmann/Schlender/Stentzel/Veil, DSGVO, 2018, Rz. 42 ff. zu Art. 26.

> rules, and on the other hand that the multiplication of controllers may also lead to undesired complexities and to a possible lack of clarity in the allocation of responsibilities. This would risk making the entire processing unlawful due to a lack of transparency and violate the principle of fair processing.“[18]

Die Art.-29-Datenschutzgruppe macht hier deutlich, dass gerade komplexe Verarbeitungssituationen die Gefahr bergen, dass es zu Lücken im Schutz der Betroffenen kommt, weil niemand sich zuständig fühlt. Dabei verweist das Papier auf die Gefahr der Intransparenz und die Verletzung des Grundsatzes erwartbarer, fairer, Datenverarbeitung (jetzt in Art. 5 Abs. 1 DSGVO Grundpflicht).

Für die betroffenen Patienten entsteht durch die ärztliche „Verschreibung“ der CGM-Cloud und das Auslesen der Daten durch die Praxis eine u.U. lebenswichtige und enge Verbindung von CGM-Anbieter und ärztlichem Behandler. Dabei ist die reale Ansprechperson der ärztliche Behandler. Nach bisherigem Verständnis soll dieser allerdings mit der CGM-Cloud gar nichts zu tun haben. Der CGM-Cloud-Anbieter, der die Daten tatsächlich speichert ist — weil Massengeschäft — nicht in der Form persönlich ansprechbar wie die behandelnde Ärztin oder der behandelnde Arzt.

Diese Situation führt aber genau zu der Art von Intransparenz, die nach Art. 5 Abs. 1 lit. a) DSGVO zur Rechtswidrigkeit der ganzen Verarbeitung führen kann. Eine formelhafte Freizeichnung von Verantwortung durch den ärztlichen Behandler, für eine Form der Datenspeicherung, von der er selbst profitiert, widerspricht der berechtigten Erwartung der Patienten und damit dem Prinzip der Verarbeitung nach Treu und Glauben (Art. 5 Abs. 1 lit. a) DSGVO).[19]

Es ist also davon auszugehen, dass das bisherige Nebeneinander der Verarbeitung der Messdaten durch CGM-Cloud-Anbieter und ärztlichen Behandler den einzuhaltenden und im Zweifel zu beweisenden Grundsätzen des Art. 5 DSGVO widerspricht.

Folgerichtig hat daher die Datenschutzgruppe schon in ihrem Papier von 2010 unter Beispiel 15 eine öffentlich-rechtlich betriebene Plattform, zum Austausch von Patientendaten, als gemeinsame Verarbeitung eingeordnet.[20]

18 Art.-29-Datenschutzgruppe, 00264/10/EN WP 169, Opinion 1/2010 on the concepts of "controller" and "processor", p. 22,23.

19 So auch Gierschmann/Schlender/Stentzel/Veil, DSGVO, 2018, Rz. 12 zu Art. 26; Martini in: Paal/Pauly, DSGVO/BDSG, 2. Aufl., 2018, Rz. 1 zu Art. 26: „transparente Verantwortungsstrukturen“; so auch Sydow (Hrsg.), DSGVO, 2018, Rz. 1 zu Art. 26.

20 Example No. 15: Platforms for managing health data
In a Member State, a public authority establishes a national switch point regulating the exchange of patient data between healthcare providers. The plurality of controllers - tens of thousands - results in such an unclear situation for the data subjects (patients) that the protection of their rights would be in danger. Indeed, for data subjects it would be unclear whom they could address in case of complaints, questions and requests for

E. Empfehlungen zum weiteren Vorgehen

I. Keine Verwendung der Mustervorlage

Die Verwendung der Mustervorlage (Anlage 1) wird ausdrücklich nicht empfohlen.

Wie oben dargelegt, bedarf es der in Absatz 3 vom Patienten hier eingeforderten Einwilligung nicht. Zudem sind die technischen Erläuterungen wenig hilfreich für die Patienten. Der schlichte Verweis auf die Datenschutzerklärungen der CGM-Cloud-Anbieter ist nicht ausreichend, da eine gemeinsame Verantwortlichkeit nach Art. 26 DSGVO für die Datenverarbeitung vorliegt.

Beim Bestehen einer solchen gemeinsamen Verantwortlichkeit nach Art. 26 DSGVO müssen die Beteiligten, also die jeweiligen ärztlichen Behandler und die jeweiligen CGM-Anbieter, nach Art. 26 Abs. 1 Satz 2 DSGVO in einer Vereinbarung festlegen, wer jeweils welche Verpflichtungen nach der DSGVO erfüllt. Hierbei ist insbesondere klar zu regeln, wie die Wahrung der Betroffenenrechte sichergestellt wird und wer, in welcher Form, der Erfüllung einzelner Informationspflichten nach den Artikeln 13 und 14 DSGVO nachkommt.

Dieses Ergebnis wird weder bei den Ärzten und Ärztinnen, noch bei den CGM-Cloud-Anbietern auf große Zustimmung stoßen. Beide Gruppen müssen nämlich etwas mehr tun als bisher. Auf der anderen Seite müssen neue Risiken für die Gesundheitsdaten der Patienten von allen Akteuren frühzeitig erkannt und minimiert werden. In einem zunehmend digital vernetzten und hoch arbeitsteilig Gesundheitsdaten verarbeitenden Gesundheitssystem muss für alle Beteiligten und insbesondere für die Patienten die Transparenz der Vorgänge oberste Priorität haben. Nur so ist das therapeutisch wichtige Vertrauen der Patienten zu erhalten. Für den Patienten ist es daher entscheidend, vor Ort in der Praxis auch Fragen zu Cloudspeicherung stellen zu dürfen. Durch eine verbindliche Regelung zwischen CGM-Cloud-Anbietern und „Praxen“ können auf Seiten der CGM-Cloud-Anbieter kompetente Ansprechpartner benannt werden, an die die Patienten von den Praxen unproblematisch und verbindlich verwiesen werden können.

---

information, corrections or access to personal data. Furthermore, the public authority is responsible for the actual design of the processing and the way it is used. These elements lead to the conclusion that the public authority establishing the switch point shall be considered as a joint controller, as well as a point of contact for data subjects' requests. A.a.O. p. 24.

So können die ärztlichen Behandler jederzeit sicher sein, dass ihre Patienten zeitnah weiterführende Auskünfte erhalten und die durch die Europäische Grundrechtecharta in Art. 8 Abs. 2 besonders geschützten Betroffenenrechte jederzeit und unmittelbar wahrnehmen können.

II. Auswirkungen des Urteils des EuGH vom 16.7.2020 – Schrems II auf das Ergebnis des Gutachtens

Der Gerichtshof der Europäischen Union (EuGH) hat in seiner Entscheidung vom 16.7.2020, in der Rechtssache C-311/18, Schrems II, unter anderem das seit rund vier Jahren bestehende Privacy Shield Abkommen[21] der Europäischen Union (EU) mit den Vereinigten Staaten von Amerika (USA) für ungültig erklärt. Da das Urteil leider keine Übergangsfrist enthält sind damit de jure ab 16.7.2020 alle nur auf dem Privacy Shield basierenden Datentransfers in die USA rechtswidrig.

Hier könnte man meinen, damit hätte sich das Thema CGM-Cloud rechtlich „erledigt“ und damit auch das vorliegende Gutachten.

Tatsächlich ist dies nicht so. Die DSGVO sieht ein abgestuftes System von Absprachen vor, die alle darauf abzielen im Drittland ein der EU gleichwertiges Schutzniveau zu erzeugen. Der hier im Urteil in Frage stehende Angemessenheitsbeschluss bezüglich des Privacy Shields ist nur eine, in Art. 45 DSGVO genannte Möglichkeit der rechtmäßigen Datenübertragung in ein Drittland. es können aber andere, geeignete Garantien eine Datenübertragung ermöglichen. So können bspw. auch Standardvertragsklauseln nach Art. 46 DSGVO eingesetzt werden, bindende Unternehmensregeln und sonstige weitere Garantien können geschaffen und zur Genehmigung vorgelegt werden. Speziell für die USA wird es hier zentral auf die Frage ankommen, ob der Datenempfänger Eingriffsbefugnissen der US-Geheimdienste etwa aufgrund von § 702 FISA unterliegt. Selbst wenn keinerlei sonstige Garantie iSd. Art. 45 ff. DSGVO bestünden, käme bezüglich der CGM-Clouds immer noch die Einwilligung nach Art. 9 DSGVO bzw. soweit die Betroffenen diese aus physischen oder rechtlichen Gründen nicht abgeben können eine Zulässigkeit aus Art. 49 Abs. 1 lit. f) DSGVO (Übermittlung zum Schutz lebenswichtiger Interessen) in Betracht.

Es ist sehr unwahrscheinlich, dass der Datenschutz die CGM-Cloud rechtlich unmöglich macht. Die vom EuGH nicht eingeräumte Übergangsfrist, wird sicher de facto von den Behörden gewährt werden, damit eine rechtlich vertretbare Lösung gefunden werden kann. Die Kommission überarbeitet gerade die

21 Angemessenheitsbeschluss der Kommission (EU) 2016/1250 vom 12.7.2016.

Standardvertragsklauseln, die der EuGH in seinem Urteil ausdrücklich erwähnt und hervorhebt. Zudem hat der EuGH die Möglichkeit eröffnet diese Standardvertragsklauseln mit weiteren Garantien anzureichern.

Das Urteil des EuGH schaltet die CGM-Clouds also gerade nicht automatisch ab. Die CGM-Cloud-Anbieter werden dies auch nicht von sich aus tun. Die deutschen Datenschutzbehörden werden ebenfalls sicher nicht zeitnah unkoordiniert Untersuchungen starten und Untersagungen aussprechen.

Die CGM-Cloud ist also nicht „erledigt“. Im Gegenteil: Das Schrems II-Urteil zeigt, dass auch ein Patient jederzeit ein Urteil zur CGM-Cloud erwirken kann. Je besser die Beteiligten auf ein solches Szenario vorbereitet sind, desto besser. Neben der oben festgestellten gemeinsamen Verantwortlichkeit nach Art. 26 DSGVO, besteht nach Art. 20 DSGVO auch eine Verpflichtung der CGM-Cloud-Anbieter die Daten auf Wunsch der Betroffenen in einem medienneutralen Format herauszugeben, ja diese auf Wunsch an eine andere CGM-Cloud weiterzuleiten (Stichwort: Datenportabilität). Auch dies muss mit den CGM-Cloud-Anbietern erörtert werden. Sicher nicht im Sinne einer strikten Forderung, sondern zunächst im Sinne eines gemeinsamen Rechtsgesprächs. Ein solches Gespräch hat ja am 22. August 2017 sehr erfolgreich im Langenbeck-Virchow-Haus in Berlin stattgefunden.

III. Roundtable-Workshop nach Art des „Code of Conduct Treffens“ vom 22.8.2017 in Berlin

Einer Fachgesellschaft wie der DDG wächst hier für den Datenschutz eine weitere, sehr bedeutende Rolle zu. Anders als die Beteiligten, kann sie eine Plattform bilden, um die Interessen ihrer Mitglieder aber auch der CGM-Cloud-Anbieter und der Patienten zu benennen und in praktikablen Lösungsvorschlägen zum Ausgleich zu bringen. Dies ist gerade für den Datenschutz von Gesundheitsdaten in komplexen Verarbeitungssachverhalten sehr wichtig.

Die DDG sollte daher in einem nächsten Schritt auf die CGM-Anbieter zugehen und — wenn nicht schon die Rahmenbedingungen für die nach Art. 26 DSGVO notwendigen Vereinbarungen mit den Arztpraxen aushandeln — so doch die Rechtsmeinung zur CGM-Cloud darlegen. Ebenso ist das Thema der Datenportabilität zu erörtern. Bestenfalls kann sodann eine Mustervereinbarung erarbeitet werden, die für die Praxen und alle derzeit am Markt vertretenen Unternehmen gut handhabbar sein wird. Andernfalls sind jedenfalls alle Beteiligten entsprechend sensibilisiert.

Anlage 1

Text der Mustererklärung 3.2.2020 (BVND)

Nutzung von Online Anwendungen zum Datentransfer der Glukosesensoren und Insulinpumpen in der Praxis xxx

Sehr geehrte/r Frau/Herr xxxx, geb. am xxx,

Für Ihre System xxxx,

stellt der Hersteller eine Anwendung im Internet (Cloud) zur Verfügung. Um den Datentransfer für Sie so einfach wie möglich zu gestalten, bieten wir an, Ihr o.g. System mittels unseres eigenen Zuganges zur Software von xxxx auszulesen.

Wir weisen aber darauf hin, dass dadurch Ihre Daten an den Hersteller u.a. in die USA weitergeleitet werden. Wir haben keinen Einfluss auf die Sicherheit der Verarbeitung bei diesem Hersteller. Nähere Informationen sollten Sie aber in den Datenschutzhinweisen des Herstellers finden.

Ich bin mit der Nutzung der Onlinesoftware durch die Praxis einverstanden.Meine Einwilligung kann ich in der Praxis jederzeit widerrufen. In dem Fall würden meine Daten im System des Herstellers wieder gelöscht werden.

Praxisort, den xxx Unterschrift

Anlage 2

Anbieterliste (Stand Juli 2020):

Firma	***Name Sensor***
Abbott	Freestyle Libre
Dexcom	G4, G5, G6, Clarity
Senseonics (lizensiert an Roche)	Eversense CGM, Smart Pics Software (Senovo)
Medtronic	Enlite, Guardian
Menarini	Glucoday, Glucomen