Whitepaper

SKW Schwarz

Oktober 2023

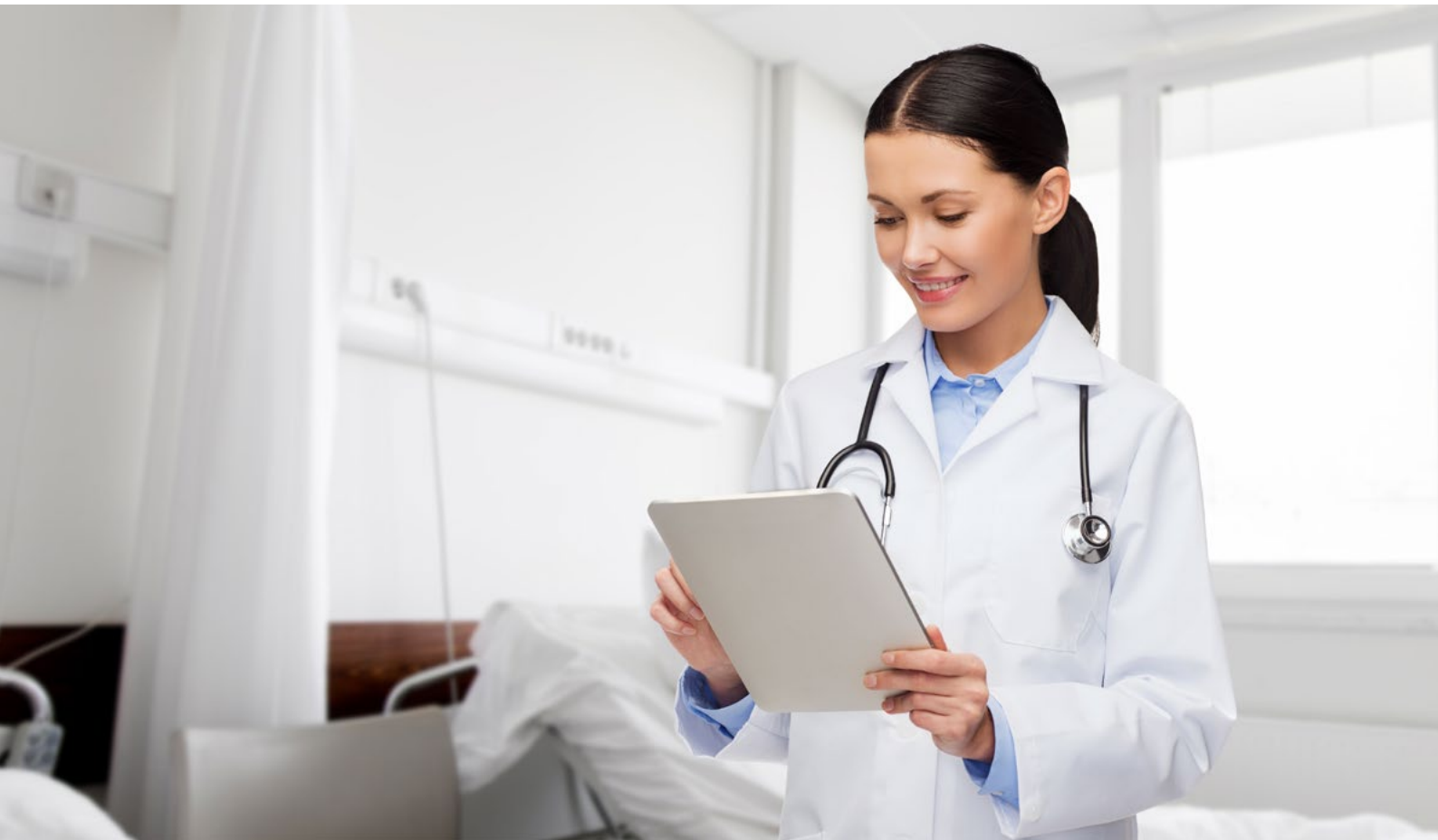
Datenschutz beim Einsatz von Medizinprodukten

Inhalt

A. Einleitung

Ob Röntgen- oder Ultraschallgeräte, Herzschrittmacher oder Gesundheits-Apps: Längst sind Medizinprodukte ein fester Bestandteil der Patientenbehandlung und spielen eine immer größere Rolle bei der Erbringung von Gesundheitsdienstleistungen. Für die Weiterentwicklung dieser Produkte spielt insbesondere auch das Thema der Digitalisierung eine zunehmend bedeutende Rolle, da diese vermehrt mit digitalen Funktionen ausgestattet werden. Dieser digitale Fortschritt ist allerdings auch mit neuen Herausforderungen in Bezug auf den Datenschutz und die Datensicherheit verbunden: Der Einsatz solcher Produkte hat nämlich die Verarbeitung einer großen Menge an personenbezogenen Daten zur Folge. Um diese Daten ausreichend zu schützen, müssen sich die betroffenen Akteure, allen voran Hersteller und Anwender, an datenschutzrechtliche Vorschriften halten. Denn so wichtig wie die medizinische Behandlung auch ist, der Schutz personenbezogener Daten darf hierbei nicht außer Acht gelassen werden.

Was müssen also Hersteller im Hinblick auf den Datenschutz bei der Entwicklung von Medizinprodukten berücksichtigen und worauf müssen Anwender beim Einsatz dieser medizinischen Produkte achten, um die Daten der betroffenen Personen ausreichend zu schützen? Diese und weitere Fragen sind Gegenstand des nachfolgenden Whitepapers und sollen näher beleuchtet werden.



B. Medizinprodukte

I. Definition

Um die datenschutzrechtliche Problematik zu verstehen, muss zunächst die Frage geklärt werden, was unter einem Medizinprodukt überhaupt zu verstehen ist. Der Begriff Medizinprodukt ist in der Medizinprodukteverordnung (nachfolgend „**MDR**“) unter Art. 2 Abs. 1 MDR definiert und meint alle Produkte, die vom Hersteller dazu bestimmt sind, Krankheiten und Verletzungen von Patienten zu diagnostizieren, zu überwachen, zu lindern und zu therapieren.

Hierzu heißt es in Art. 2 Abs. 1 MDR:

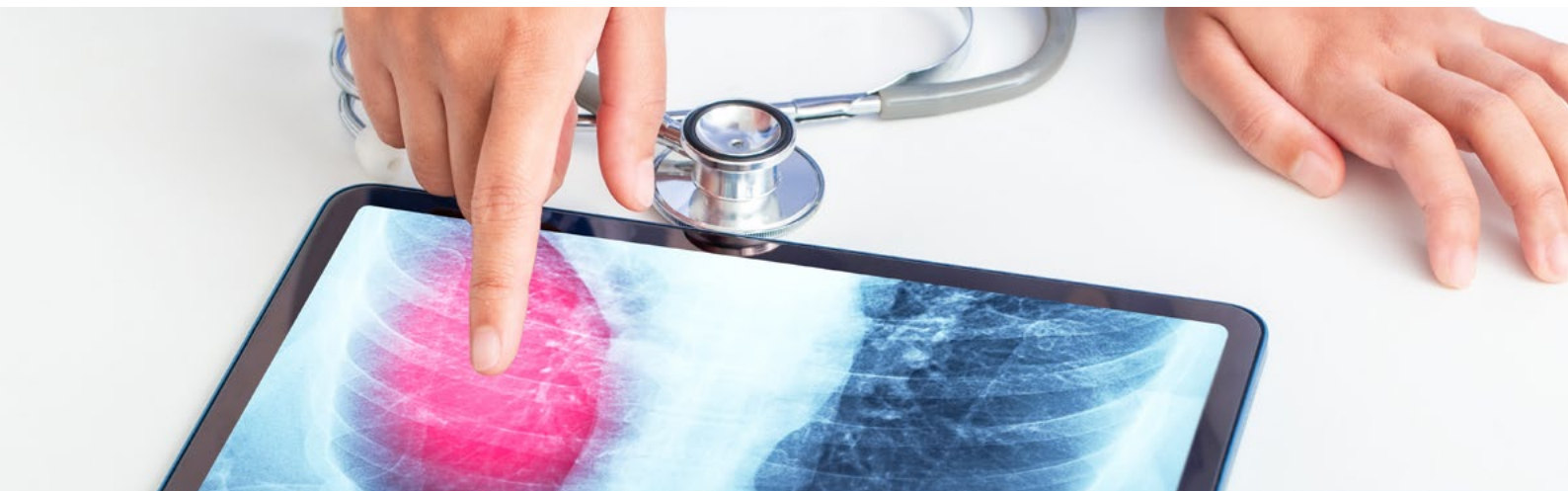
„Ein Medizinprodukt bezeichnet ein Instrument, einen Apparat, ein Gerät, eine Software, ein Implantat, ein Reagenz, ein Material oder einen anderen Gegenstand, das dem Hersteller zufolge für Menschen bestimmt ist und allein oder in Kombination einen oder mehrere der folgenden spezifischen medizinischen Zwecke erfüllen soll:

- Diagnose, Verhütung, Überwachung, Vorhersage, Prognose, Behandlung oder Linderung von Krankheiten,
- Diagnose, Überwachung, Behandlung, Linderung von oder Kompensierung von Verletzungen oder Behinderungen,
- Untersuchung, Ersatz oder Veränderung der Anatomie oder eines physiologischen oder pathologischen Vorgangs oder Zustands,
- Gewinnung von Informationen durch die In-vitro-Untersuchung von aus dem menschlichen Körper — auch aus Organ-, Blut- und Gewebespenden — stammenden Proben

und dessen bestimmungsgemäße Hauptwirkung im oder am menschlichen Körper weder durch pharmakologische oder immunologische Mittel noch metabolisch erreicht wird, dessen Wirkungsweise aber durch solche Mittel unterstützt werden kann.“

Der Wortlaut der MDR macht also deutlich, dass es für die Qualifizierung als Medizinprodukt grundsätzlich auf die Zweckbestimmung ankommt.

Medizinprodukte werden in die vier Risiko-Klassen I, IIa, IIb und III nach MDR unterteilt.



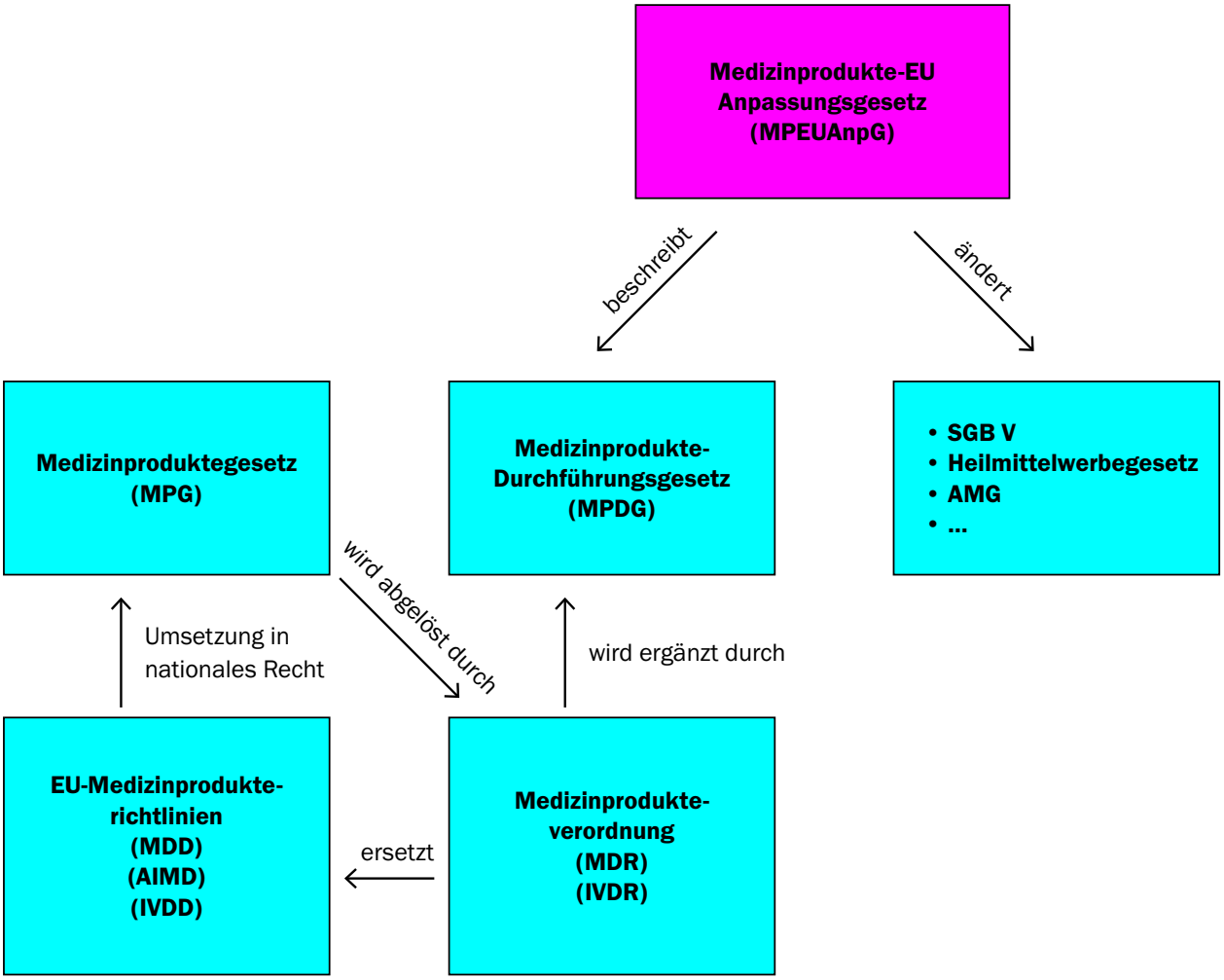
II. Beispiele

Medizinprodukte (+)	**Medizinprodukte (-)**
• **Klasse I: Geringes Risiko** z.B.: Lesebrille, Rollstühle, Fieberthermometer • **Klasse IIa: Mittleres Risiko** z.B.: Hörgeräte, Ultraschallgeräte, Röntgenfilme • **Klasse IIb: Hohes Risiko** z.B.: Röntgengeräte, Infusionspumpen • **Klasse III: Sehr hohes Risiko** z.B.: Hüft-und Kniegelenkimplantate, Herzkatheter, Brustimplantate	• Arzneimittel • Krankenhaus-Informations-systeme, sofern diese nur das Patientenmanagement unterstützen (wie Termin-planung oder Versicherungs- und Abrechnungszwecke) Herzkatheter, Brustimplantate

III. Gesetze und Verordnungen

Für Hersteller, Betreiber und sonstige Akteure von Medizinprodukten ist seit dem 26.05.2021 das Medizinprodukte-Durchführungsgesetz (nachfolgend „**MPDG**“) verbindlich. Hierbei ergänzt das MPDG die MDR und die EU-Verordnung für In-vitro-Diagnostika (EU) 2017/746 (In-vitro Diagnostics Regulation, nachfolgend „**IVDR**“) um nationale Vorgaben. Das MPDG hat das bis dahin geltende Medizinproduktegesetz (nachfolgend „**MPG**“) abgelöst, wobei letzteres der Umsetzung der EU-Medizinprodukterichtlinien (MDD, AIMD, IVDD) diente. Das MPDG wurde als Teil des Medizinprodukte-EU-Anpassungsgesetzes (nachfolgend „**MPEUAnpG**“) eingeführt, wobei das MPEUAnpG auch Änderungen an weiteren Gesetzes vorsieht (bspw.: SGB V, Heilmittelwerbegesetz und Arzneimittelgesetz). Das MPDG und die EU-Medizinprodukteverordnungen haben gemeinsam zum Ziel, den Umgang mit Medizinprodukten im Hinblick auf das Inverkehrbringen und die Inbetriebnahme zu regeln und damit für die Sicherheit, Eignung und Leistung der Produkte zu sorgen und ausreichenden Schutz für Patienten, Anwender und Dritte zu gewährleisten.

Zur Veranschaulichung der wichtigsten Regelungen soll das folgende Schaubild dienen:



IV. Hersteller von Medizinprodukten

Wenn über Medizinprodukte und Datenschutz gesprochen wird, stellt sich in erster Linie die Frage, welche Akteure in der Kette überhaupt in der Pflicht stehen, die Daten von betroffenen Personen beim Einsatz von Medizinprodukten im Sinne der DS-GVO sowie weiterer Begleitgesetze zu schützen.

Auf den ersten Blick scheint die Antwort klar auf der Hand zu liegen: Anwender von Medizinprodukten, wie etwa Kliniken oder Arztpraxen, sind originär für die Einhaltung des Datenschutzes verantwortlich. Schließlich sind sie diejenigen, welche die Daten von Patienten zu Zwecken deren Behandlung oder Überwachung erheben, verarbeiten und anschließend aufbewahren.

Doch so einfach wie es auf den ersten Blick scheint, ist es in der Praxis häufig nicht. Schaut man sich nämlich die Anforderungen der Datenschutz-Grundverordnung (nachfolgend „**DS-GVO**“ genannt) genauer an, so kristallisiert sich ein weiterer Akteur in der Kette heraus: Der Hersteller von Medizinprodukten (nachfolgend „**Hersteller**“ genannt). Zwar ist es zutreffend, dass Hersteller nur in gewissen Konstellationen Verantwortliche im Sinne der DS-GVO sind und damit in den "klassischen" Anwendungsfällen von Medizinprodukten - insbesondere sofern es um die "bloße" Bereitstellung des Medizinprodukts geht - keine umfassenden datenschutzrechtlichen Verpflichtungen wie ein Verantwortlicher, zum Beispiel die Durchführung einer Datenschutz-Folgenabschätzung, haben. Allerdings treten sie insoweit regelmäßig als Auftragsverarbeiter auf und müssen in diesem Zusammenhang ebenfalls einigen Verpflichtungen aus der DS-GVO nachkommen, etwa das Führen eines Verarbeitungsverzeichnisses nach Art. 30 Abs. 2 DS-GVO (siehe hierzu Gliederungspunkt IV. 5).

Darüber hinaus haben Hersteller ein großes Interesse daran, ihre Produkte nach Fertigstellung auf dem Markt einem möglichst breiten Publikum anzubieten. Damit ihnen das auch gelingt, sollten Sie dringend darauf achten, Anwendern von Medizinprodukten (nachfolgend „**Anwender**“ genannt) die Umsetzung des Datenschutzes später beim Einsatz dieser Produkte zu erleichtern. Dies kann in Anlehnung an Art. 25 DS-GVO bereits im Rahmen der Produktentwicklungsphase berücksichtigt werden. Während Abs. 1 die datenschutzfreundliche Technikgestaltung (sog. **Privacy by Design**) betrifft, regelt Abs. 2 die datenschutzfreundlichen Voreinstellungen des Medizinproduktes (sog. **Privacy by Default**). Privacy by Design meint, dass das Produkt datenschutzfreundlich gestaltet sein muss. Das heißt, dass für das konkrete Produkt risikobasierte, effektive und angemessene technische sowie organisatorische Maßnahmen ergriffen werden müssen, um die Rechte der betroffenen Personen weitestgehend zu schützen. Privacy by Default hingegen betrifft die Voreinstellungen des Medizinproduktes. Diese müssen im Hinblick auf den Grundsatz der Datenminimierung so gestaltet sein, dass nur solche Daten verwendet werden, welche für die jeweiligen Verarbeitungszwecke auch erforderlich sind. Welche konkreten Maßnahmen bei der Entwicklung letztendlich ergriffen werden sollten, gibt Art. 25 DS-GVO nicht vor. Die Vorschrift ist bewusst abstrakt gehalten und gibt viel Spielraum, um auf diese Weise technologieneutral zu bleiben und sich den technischen Entwicklungen anpassen zu können. Insofern sollten Hersteller das eigene Produkt durch die Datenschutz-Brille des Kunden betrachten. Eine Win-Win-Situation für beide Seiten: Während Hersteller potentiellen Kunden datenschutzkonforme und attraktive Produkte anbieten können und so ihre Verkaufschancen auf dem Markt ankurbeln, wird Anwendern die Erfüllung ihrer datenschutzrechtlichen Anforderungen um ein Vielfaches erleichtert. Für Hersteller sollte insofern der Datenschutz und die Datensicherheit im Rahmen der Produktentwicklung hohe Priorität haben. Weitere datenschutzrechtliche Anwendungsfälle aus Sicht von Herstellern sind die Durchführung von klinischen Prüfungen (vor und nach dem Inverkehrbringen des Produktes) sowie die Forschung und Qualitätssicherung zu eigenen Zwecken (abseits von regulatorischen Anforderungen). Die zuletzt genannten Fälle sind jedoch - auch in datenschutzrechtlicher Hinsicht - sehr speziell, weshalb diese nicht im Fokus des vorliegenden Whitepapers stehen sollen. Nachstehend sollen demgegenüber gerade "klassische" datenschutzrechtliche Fragestellungen beantwortet werden, welche beim Bereitstellen einer entsprechenden Anwendung typischerweise aufkommen. Auch sind weitergehende rechtliche Anforderungen natürlich dann möglich, sofern es sich nicht um das hier adressierte klassische 3-Personen-Verhältnis (Patient, Anwender und Hersteller) handelt.

Unabhängig davon, ob es sich nun um Hersteller oder Anwender von Medizinprodukten handelt, müssen jedenfalls sämtliche der in Art. 5 Abs. 1 DS-GVO dargelegten datenschutzrechtlichen Grundsätze beachtet werden. Hierzu gehören die Rechtmäßigkeit der Datenverarbeitung, die Zweckbindung, die Datenminimierung, die Transparenz, die Datenrichtigkeit, die Speicherbegrenzung, der Grundsatz der Datensicherheit und die Rechenschaftspflicht.

Wie das Ganze nun konkret aussehen kann und worauf Hersteller besonders achten sollten, wird nachfolgend im Einzelnen aufgezeigt.

1. Technische Umsetzung

Im Rahmen der Entwicklungsphase sollten Hersteller in technischer Hinsicht gewisse Funktionalitäten in ihre Medizinprodukte implementieren, um Anwender bei der Einhaltung der Datenschutzregeln zu unterstützen. Folgende Punkte sollten daher bereits von Beginn an im Rahmen der Entwicklungsphase berücksichtigt werden:

a) Verschlüsselung

→ Hersteller sollten sicherstellen, dass die Kommunikation bzw. die Datenübertragung über Schnittstellen zwischen dem jeweiligen Medizinprodukt und anderen technischen Systemen sowie die anschließende Datenspeicherung (insbesondere im Falle von cloudbasierten Tools) in verschlüsselter Form erfolgt. Damit das jeweilige Produkt für den Anwender „attraktiv“ ist, sollten die Daten im gesamten Lebenszyklus – nach dem Stand der Technik – abgesichert sein.

b) Berechtigungskonzept

→ Darüber hinaus sollten Hersteller im Rahmen der Produktentwicklung darauf achten, ein detailliertes Berechtigungskonzept zu ermöglichen und so einen datenschutzkonformen Einsatz zu gewährleisten. Die jeweiligen zu verarbeitenden personenbezogenen Daten erfahren auf diese Weise einen hohen Schutzstatus, da nur solche Mitarbeiter Zugriff auf das Medizinprodukt erhalten, welche aktiv autorisiert wurden. Für den Fall, dass ein Mitarbeiter im Nachgang doch noch mehr Rechte benötigen sollte, sollten sich die notwendigen Anpassungen bei Bedarf bewusst und im erforderlichen Maße vornehmen lassen.

c) Clusterung des Storagesystems

→ Ferner sind Hersteller auch gut beraten, im Hinblick auf die Speicherung der jeweiligen Daten bei Medizinprodukten eine Clusterung des Storage-Systems sicherzustellen und dadurch die Daten auf verschiedene Systeme zu verteilen. Hierzu folgendes Beispiel: Ein Krankenhaus verwendet ein clusterbasiertes Röntgengerät. Die von diesem Röntgengerät aufgenommenen medizinischen Bilder werden nicht lokal auf dem Gerät gespeichert, sondern auf mehrere Speicherknoten im Netzwerk repliziert. Wenn nun ein Server aufgrund eines Hardwarefehlers oder einer Naturkatastrophe ausfällt, sind die Bilder noch auf den anderen Servern verfügbar. Dadurch wird gewährleistet, dass die medizinischen Daten nicht verloren gehen und die Patientenversorgung kontinuierlich gewährleistet ist. Insofern bietet die Clusterung von Medizinprodukten eine erhöhte Ausfall- und Datensicherheit, um die Integrität der gespeicherten Daten zu gewährleisten.

d) Archivformat

→ Im Hinblick auf die Archivierung der Daten sollte das Archivformat insgesamt so angelegt werden, dass die Lesbarkeit der Daten auch in Zukunft sichergestellt ist. Hierfür sollten Hersteller insbesondere offene Standards verwenden, welche von einem breiten Publikum unterstützt werden. So stellt etwa DICOM (Digital Imaging and Communications in Medicine) einen weit verbreiteten offenen Standard für die Übertragung und Speicherung von medizinischen Bildern und den dazugehörigen Informationen dar. DICOM wird von medizinischen Bildgebungsgeräten wie Röntgengeräten, CT-Scannern und Ultraschallgeräten verwendet, um Bilder in einem standardisierten Format zu speichern und auszutauschen sowie den Zugriff auf diese medizinischen Daten zu gewährleisten. Darüber hinaus sollten Hersteller auch umfassende Dokumentationen dazu bereithalten, wie bspw. das Archivformat aufgebaut ist und auf welche Weise darauf zugegriffen werden kann.

e) Fernwartung

→ Für den Fall, dass externe Dienstleister die Fernwartung für Medizinprodukte übernehmen, sollte bei der Entwicklung des Medizinproduktes ein besonderes Augenmerk daraufgelegt werden, dass diesen Dienstleistern gegenüber keine personenbezogenen Daten offengelegt werden (Grundsatz der Datenminimierung). Der Zugriff sollte sich – sofern möglich – nur auf die Offenlegung von technischen Daten beschränken. Hierfür sollten die personenbezogenen Daten sowie die technischen Daten bereits im Vorfeld im Rahmen der Produktentwicklung in getrennten Tabellen aufbewahrt werden. Da Hersteller in der Regel die Fernwartung übernehmen, sollten diese daher gegenüber den Anwendern transparent darlegen, auf welche konkreten Daten sie Zugriff haben und wie die einzelnen Datenströme aufgebaut sind. Sofern die Zugriffsmöglichkeit nicht eingeschränkt werden kann, sollte alternativ bspw. an eine Pseudonymisierung der gespeicherten Daten gedacht werden, sodass auf diese Weise kein Personenbezug hergestellt werden kann. Ferner sollte sichergestellt werden, dass stets vor Beginn der Fernwartungsarbeiten der jeweilige Anwender dem Dienstleister eine (digitale) Zugriffsberechtigung erteilt. Solange also eine solche Berechtigung nicht erteilt wurde, besteht für den Dienstleister keine Möglichkeit, auf das Medizinprodukt und damit auf die Daten zuzugreifen.

f) Löschung

→ Hersteller sollten in Anlehnung an den Grundsatz der Speicherbegrenzung auch sicherstellen, dass eine Löschung von einzelnen Daten zu verschiedenen Zeitpunkten automatisiert ermöglicht wird. In diesem Zusammenhang bietet sich die Implementierung eines automatisierten Löschkonzeptes an. Sollte dies aus technischen Gründen nicht möglich sein, wäre alternativ eine Anonymisierung der Daten im System zu integrieren, um dadurch die Herstellung eines Personenbezuges zu unterbinden. Hierbei muss jedoch natürlich beachtet werden, dass eine Anonymisierung strengen datenschutzrechtlichen Anforderungen unterliegt. Das Verfahren muss daher dazu geeignet sein, dass niemand (also weder Anwender noch Hersteller) mit verhältnismäßigem Aufwand dazu in der Lage sind, einen Personenbezug (wieder-)herzustellen.

g) Aktualisierungen und Sicherheitspatches

→ Hersteller sollten darüber hinaus regelmäßige Updates und Sicherheitspatches zur Verfügung stellen, um Schwachstellen und Sicherheitslücken zu schließen. Sie kennen ihre Produkte im Zweifel am besten und bringen insofern das notwendige Know-how mit, um entsprechende Produkte zu entwickeln und entsprechend einzusetzen. Auf diese Weise können Anwender sicherstellen, dass Ihre Produkte auf dem aktuellsten Stand sind, um etwaigen Datenschutzvorfällen von vornherein zu begegnen.

h) Unterstützung bei Datenschutz-Audits

→ Eine weitere wichtige Unterstützung können Hersteller dahingehend leisten, dass sie ihre Kunden bei der Durchführung von Datenschutz-Audits unterstützen. Eine wesentliche Hilfestellung können hierbei die Zurverfügungstellung von Informationen und Dokumentationen bieten, welche für solche Prüfungen benötigt werden.

2. Bereitstellung von Datenschutzinformationen

Wie bereits eingangs erläutert, sind - in der hier beleuchteten Konstellation - regelmäßig die Anwender als Verantwortliche zur Einhaltung der in der DS-GVO niedergelegten formellen Anforderungen verpflichtet. Um diesen Anforderungen auch ordnungsgemäß nachkommen zu können, benötigen Anwender hierfür einige wichtige Informationen. So müssen Anwender etwa im Rahmen der Durchführung einer Datenschutz-Folgenabschätzung die Datenflüsse im Zusammenhang mit dem Medizinprodukt verstehen, um auf dieser Basis bewerten zu können, ob hohe Risiken für die Rechte der betroffenen Personen bestehen. In diesen Fällen können Hersteller Hilfestellungen bieten und für mehr Transparenz sorgen, zumal letztlich die Hersteller über das nötige Know-how verfügen. In der Regel ist es nämlich so, dass die Medizinprodukte bereits einen gewissen Datenumfang aufgrund der mitgelieferten Funktionalität vorgeben bzw. implizieren. Hersteller sollten daher neben dem Medizinprodukt noch weitere Dokumente, etwa in Form von FAQs oder eines Whitepapers mit Datenschutzinformationen für ihre Kunden bereithalten, woraus bspw. hervorgeht, wie personenbezogene Daten von dem Medizinprodukt erfasst, verarbeitet, gespeichert und geschützt werden. Darüber hinaus sollte eine ausführliche Beschreibung der jeweiligen Datenflüsse erfolgen. Insofern ist es regelmäßig sinnvoll, solche Musterdokumente zu entwerfen und den Kunden zur Verfügung zu stellen. Nur so kann schließlich sichergestellt werden, dass Anwender ihrerseits ihren Pflichten aus der DS-GVO ordnungsgemäß nachkommen können.

Wichtig:

Sollte der Hersteller eines Medizinprodukts die jeweiligen Daten auch zu eigenen Zwecken verarbeiten (müssen), sollten auch diese Informationen bereits in ein entsprechendes Muster-Dokument eingearbeitet werden. Insbesondere sollte in diesen Fällen sehr gründlich geprüft werden, auf welche datenschutzrechtliche Rechtsgrundlage diese Verarbeitung zu eigenen Zwecken gestützt werden kann. Dies wird von Art und Hintergrund der Datenverarbeitung abhängen, weshalb insoweit keine pauschale Einordnung getroffen werden kann. Regelmäßig wird jedoch zu klären sein, ob eine Einwilligung des Patienten sachdienlich oder gar erforderlich ist, oder ob diese - da eine gesetzliche Rechtsgrundlage herangezogen werden kann - gerade nicht erforderlich ist. .

3. Zurverfügungstellung von Musterdokumenten

Hersteller sind vor diesem Hintergrund auch gut beraten, einige datenschutzrechtliche Musterdokumente, wie zum Beispiel einen Vertrag zur Auftragsverarbeitung, Datenschutz-Folgenabschätzungen, Datenschutzhinweise oder ein schriftliches Löschkonzept bereitzuhalten, welche auf das konkrete Produkt abgestimmt sind und potentiellen Kunden bzw. Anwendern vor dem Einsatz des Medizinproduktes zur Verfügung gestellt werden können.

4. Schulungen

Hersteller sollten ferner Anwender im Hinblick auf den Umgang mit dem jeweiligen Medizinprodukt schulen. Als Hersteller des jeweiligen Medizinproduktes bringen sie das notwendige Wissen dahingehend mit, wie das Produkt bestimmungsgemäß einzusetzen und von Anwendern zu bedienen ist. Insofern sollte die Durchführung von Schulungen ein weiterer Bestandteil ihres Angebots sein. Auf diese Weise können Datenschutzrisiken durch unsachgemäße Bedienung verringert werden. Dies kann bspw. auch die zusätzliche Bereitstellung von Schulungsmaterialien wie Bedienungsanleitungen und Leitfäden umfassen, welche Anwender darin unterstützen, bewährte Datenschutzpraktiken zu verstehen und umzusetzen.

5. Abgrenzungsproblematik

Wie bereits dargestellt, sind eine Vielzahl an Konstellationen denkbar, in denen Hersteller von Medizinprodukten personenbezogene Daten zu eigenen Zwecken verarbeiten (müssen). Dies kann bspw. im Hinblick auf die Einhaltung regulatorischer Anforderungen oder etwa zur Steigerung der eigenen Effizienz (also zur Forschung und/oder zur Qualitätssicherung) geschehen. Hersteller stehen daher regelmäßig vor der großen Frage, ob sie im Hinblick auf die Datenverarbeitung im Zusammenhang mit dem Medizinprodukt (noch) als Auftragsverarbeiter fungieren oder vielmehr - ggf. auch gemeinsam mit dem Anwender – für die Datenverarbeitung verantwortlich sind.

Auftragsverarbeiter im Sinne von Art 4 Nr. 8 DS-GVO ist jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Klassisches Merkmal hierfür ist die rein weisungsgebundene Verarbeitung zu originär "fremden" Zwecken. Von einer gemeinsamen Verantwortlichkeit hingegen ist auszugehen, wenn mindestens zwei Verantwortliche gemeinsam die Zwecke und die Mittel zur Verarbeitung festlegen. Die rechtliche Einordnung dieser Frage erweist sich im Zweifel als äußerst schwierig und hängt von diversen Faktoren ab. Sofern also Hersteller bspw. verschiedene Verarbeitungsvorgänge während dem Einsatz eines Medizinprodukts übernehmen, sollten sie stets vor Beginn der Datenverarbeitung prüfen, ob sie tatsächlich (nur) als Auftragsverarbeiter agieren. Auch sind Konstellationen denkbar, in denen verschiedene Datenverarbeitungsvorgänge differenziert zu bewerten sind. So ist es denkbar, dass die Bereitstellung von IT-Support-Leistungen der Auftragsverarbeitung unterliegt, während die anschließende Nutzung der Daten zu eigenen Zwecken in eine (ggf. gemeinsame) Verantwortlichkeit fällt. Je nachdem, welche dieser beiden Alternativen in Betracht kommt, muss der jeweilige Vertrag zwischen dem Anwender und dem Hersteller vorbereitet und unterzeichnet werden. Im Falle einer Auftragsverarbeitung ist etwa an den Abschluss eines Vertrages zur Auftragsverarbeitung zu denken.[1] Eine gemeinsame Verantwortlichkeit hingegen zieht den Abschluss eines sogenannten Joint Controller Vertrages nach sich.[2] Letzteres setzt eine detaillierte und klar verständliche Vereinbarung zwischen den Verantwortlichen voraus, etwa in Bezug auf die Frage, wer konkret welche datenschutzrechtlichen Anforderungen erfüllen muss.

Herstellern ist daher dringend anzuraten, diese Abgrenzungsproblematik bereits vor Beginn der Datenverarbeitung zu klären und zu prüfen, ob sie als Auftragsverarbeiter oder gemeinsame Verantwortliche tätig werden, um anschließend den entsprechenden Vertrag mit dem Anwender aufzusetzen und zu unterzeichnen.

6. Handlungspflichten für Hersteller

Um in datenschutzrechtlicher Hinsicht auf der sicheren Seite zu stehen, sollten Hersteller im Rahmen der Entwicklung und Zurverfügungstellung ihrer Medizinprodukte folgende drei Aspekte im Auge behalten:

- Einhaltung regulatorischer Anforderungen (insbesondere MDR, MPDG)
- Einhaltung vertraglicher Regelungen
- Einhaltung datenschutzrechtlicher Anforderungen (einschließlich § 203 StGB)

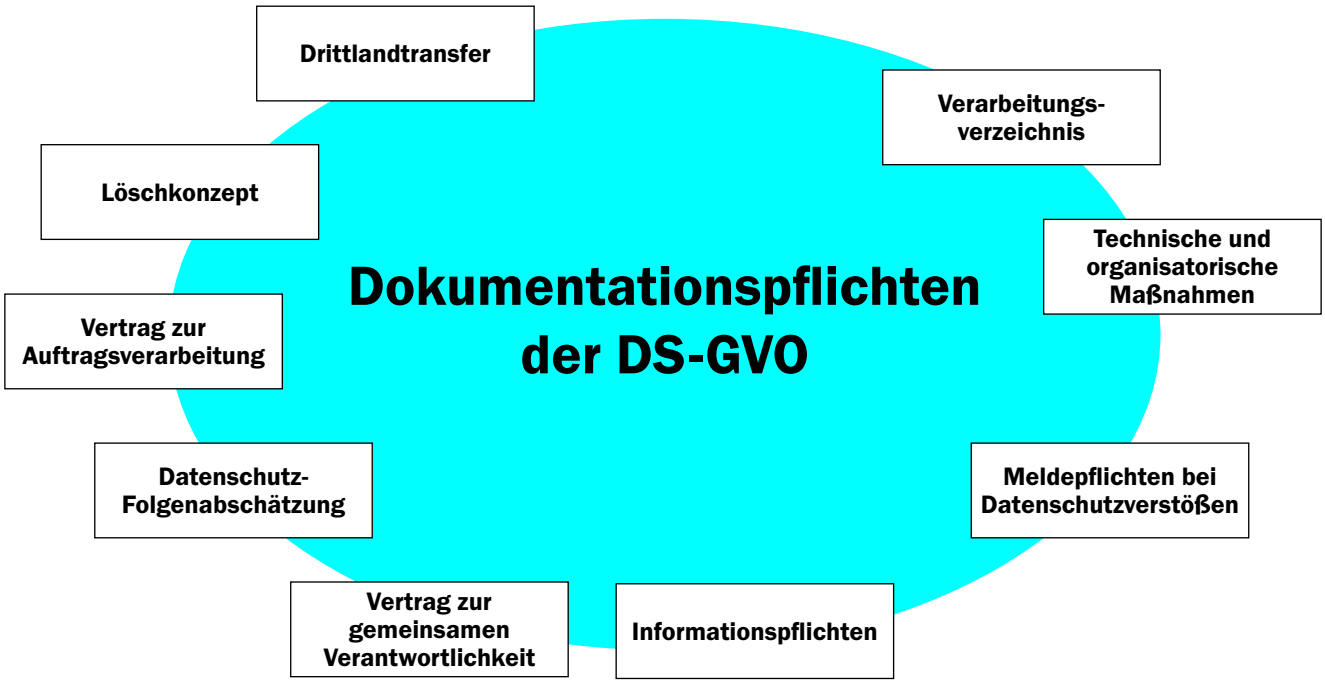
[1] https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf.

[2] https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_16.pdf.

V. Anwender von Medizinprodukten

Während Hersteller die oben aufgeführten Aspekte im Rahmen ihrer Produktentwicklung berücksichtigen sollten, sind Anwender beim Einsatz des Medizinproduktes zur Einhaltung des Datenschutzes zwingend verpflichtet (s.o.). Um einen datenschutzkonformen Einsatz von Medizinprodukten zu gewährleisten, müssen Anwender bestimmte Anforderungen erfüllen.

Zur Veranschaulichung soll folgende Grafik dienen:



Wie aus dem Schaubild entnommen werden kann, müssen Anwender zu Nachweiszwecken bestimmte formelle Anforderungen erfüllen, um ihren Dokumentationspflichten nachzukommen.

Hierzu zählen insbesondere:

Rechtsgrundlage der Datenverarbeitung

→ Zum einen müssen Anwender als verantwortliche Stelle vor dem Einsatz eines Medizinprodukts stets gründlich prüfen, welche Rechtsgrundlage für die konkrete Datenverarbeitung im Zusammenhang mit dem Medizinprodukt einschlägig ist. Hierfür kommen – je nach konkretem Anwendungsfall – mehrere Vorschriften in Betracht.

→ Zum einen besteht die Möglichkeit, die Datenverarbeitung in bestimmten Fällen auf Art. 9 Abs. 2 lit. h) DS-GVO zu stützen. Voraussetzung hierfür ist allerdings in der ersten Alternative, dass neben einem Behandlungsvertrag „mit einem Angehörigen eines Gesundheitsberufs“ - gemeint sind Ärzte sowie das bei Ärzten bzw. in Krankenhäusern beschäftigte Personal - die Datenverarbeitung ferner zu den in der Vorschrift genannten Zwecken erforderlich ist, und zwar „im Interesse einzelner natürlicher Personen und

der Gesellschaft insgesamt“. Welche Zwecke im Interesse einzelner natürlicher Personen liegen, lässt sich nicht abschließend definieren.[3] Ob diese Vorschrift im konkreten Fall tatsächlich herangezogen werden kann, etwa da es sich um einen "klassischen" Fall der Patientenbehandlung handelt, ist vom Einzelfall abhängig und muss im Vorfeld geprüft werden. Daneben sind in der zweiten Alternative des Art. 9 Abs. 2 lit. h) DS-GVO ggf. - daneben oder alternativ - auch die entsprechenden Regelungen in den Landeskrankenhausgesetzen zu beachten.

→ Möglich ist aber auch, die Datenverarbeitung auf eine datenschutzrechtliche Einwilligung nach Art. 9 Abs. 2 lit. a) DS-GVO der betroffenen Person zu stützen. Dies kann insbesondere für "atypische" Konstellationen anzunehmen sein, in denen mehr Verarbeitungsschritte vorgenommen werden, als dies für die originäre Behandlung erforderlich wäre (bspw. bei hoch-technischen Medizinprodukten mit einer Vielzahl involvierter Akteure). Für diesen Fall sollten Anwender eine entsprechende Mustereinwilligungserklärung bereithalten, welche den betroffenen Personen vor dem Einsatz des Medizinproduktes zur Unterzeichnung vorgelegt werden kann.[4] Allerdings sollten sich Anwender bei dieser Alternative darüber bewusst sein, dass im Falle eines Widerrufs eine datenschutzkonforme Löschung der Daten umzusetzen ist.

→ Als alternative Rechtsgrundlage kommt auch Art. 9 Abs. 2 lit. c) DS-GVO in Betracht. Hiernach ist die Datenverarbeitung zulässig, sofern diese zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich ist und die betroffene Person aus körperlichen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben. Gemeint sind also Notstandskonstellationen, bei denen eine mutmaßliche Einwilligung die wegen mangelnder Einwilligungsfähigkeit nicht mögliche Erklärung ersetzt.[5] Ob diese Vorschrift im konkreten Fall tatsächlich einschlägig ist, muss im Vorfeld gründlich überprüft werden, wobei Anwender in jedem Fall eine Abwägung der lebenswichtigen Interessen mit dem Datenschutz durchführen müssen. In diesen Fällen ist stets auch eine genaue Dokumentation der relevanten Umstände, die zur Einwilligungsunfähigkeit geführt haben und die die mutmaßliche Einwilligung stützen, zur Absicherung dringend anzuraten.

Verarbeitungsverzeichnis

→ Anwender sollten darüber hinaus darauf achten, das entsprechende Medizinprodukt im Verarbeitungsverzeichnis aufzuführen und die jeweiligen Informationen des Art. 30 DS-GVO darin einzutragen.[6] Hierfür sollten sie, sofern noch nicht geschehen, den Hersteller um Zurverfügungstellung der jeweiligen datenschutzrechtlichen Informationen bitten (vgl. hierzu auch Ziffer IV. 2.). Sofern Anwender mehrere Medizinprodukte in ihren Einrichtungen einsetzen und diese überwiegend ähnlich sind – etwa die gleichen Zwecke verfolgen oder auf ähnliche Daten zugreifen, können Anwender diese Medizinprodukte auch als einen gemeinsamen Prozess im Verarbeitungsverzeichnis aufführen.

Technische und organisatorische Maßnahmen[7]

→ Im Hinblick auf die Umsetzung von technischen und organisatorischen Maßnahmen können Anwender Maßnahmen, wie z.B. die Verschlüsselung und Pseudonymisierung von Daten, Zugriffskontrollen, regelmäßige Sicherheitsupdates oder die Implementierung von Firewalls ergreifen, um die Sicherheit der Daten ausreichend zu gewährleisten. Sofern Auftragsverarbeiter eingesetzt werden (bspw. im Falle einer Fernwartung), sollte auch an die Aufnahme entsprechender Regelungen im Hinblick auf die technischen und organisatorischen Maßnahmen geachtete werden.

[3] Ehmann/Selmayr/Schiff, 2. Auflage 2018, DS-GVO, Art. 9 Rn. 60.

[4] https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_20.pdf.

[5] Kühling/Buchner/Weichert, 3. Auflage 2020, DS-GVO Art. 9 Rn. 64.

[6] https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_1.pdf.

[7] https://www.datenschutzkonferenz-online.de/media/en/20191106_positionspapier_kuenstliche_intelligenz.pdf.

Meldepflichten bei Datenschutzverstößen

→ Anwender sollten stets im Auge behalten, dass es bei dem Einsatz von Medizinprodukten trotz sorgfältiger Datenschutz-Compliance zu Datenschutzvorfällen kommen kann.[8] Tritt ein solcher Fall sein, sollten Anwender auf ihr Datenschutzmanagement zurückgreifen und die darin beschriebenen Verfahrensschritte umsetzen.

Informationspflichten

→ Anwender sind ferner verpflichtet, die betroffenen Personen – meist Patienten - über die Datenverarbeitung zu informieren. Dies ist in Form von Datenschutzhinweisen umzusetzen.[9] Da regelmäßig Gesundheitsdaten verarbeitet werden, muss dies zwingend in den Datenschutzhinweisen angezeigt werden. Ferner ist darauf zu achten, die jeweiligen (externen) Datenempfänger, etwa bei der Übertragung von MRT Bildern an externe Ärzte, zu benennen. Dabei ist es im Rahmen der Informationspflichten ausreichend, Empfängerkategorien zu benennen, z.B. behandelnde Ärzte.

Datenschutz-Folgenabschätzung

→ Da im Rahmen des Einsatzes von Medizinprodukten auch Gesundheitsdaten verarbeitet werden, ist die Datenverarbeitung in der Regel mit einem hohen Risiko für die Rechte und Freiheiten der betroffenen Personen verbunden. Aus diesem Grund sollten Anwender vor dem Einsatz des Medizinproduktes in der Regel eine Datenschutz-Folgenabschätzung durchführen.[10]

Löschkonzept

→ Um dem Grundsatz der Speicherbegrenzung gerecht zu werden, muss die Einrichtung ein Löschkonzept implementieren, um sicherzustellen, dass die jeweiligen Daten nach einer bestimmten Zeit auch wieder gelöscht werden.[11] In diesem Zusammenhang bietet es sich an, bestimmte Personengruppen, wie bspw. die IT Abteilung, mit der Löschung der Daten zu beauftragen und dies im Löschkonzept entsprechend festzuhalten.

[8] https://www.datenschutz-bayern.de/datenschutzreform2018/OH_Meldepflichten.pdf.

[9] https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_10.pdf.

[10] https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf.

[11] https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_11.pdf.

Vertrag zur Auftragsverarbeitung

→ In bestimmten Fällen kann es erforderlich sein, dass Anwender im Rahmen des Einsatzes von Medizinprodukten Dienstleister einsetzen (vgl. hierzu auch Gliederungspunkt IV. 5.). Kommt der Hersteller bzw. der Anwender zu dem Ergebnis, dass die konkrete Dienstleistung einen Vertrag zur Auftragsverarbeitung zur Folge hat, so sollte im zweiten Schritt an den Abschluss eines solchen Vertrages gedacht werden. Problematisch in diesem Zusammenhang kann jedoch die Verschwiegenheitspflicht des Dienstleisters sein. Die Einhaltung der ärztlichen Schweigepflicht einerseits und die Offenlegung der Gesundheitsdaten an Auftragsverarbeiter andererseits kann im Zweifel rechtliche Probleme nach sich ziehen. Zwar sind bspw. Ärzte zunehmend bei ihrer beruflichen oder dienstlichen Tätigkeit auf die Hilfeleistung externer Dienstleister angewiesen. Sie machen sich jedoch nach § 203 Abs. 4 S. 1 Nr. 1 StGB strafbar, wenn der Dienstleister unbefugt ein fremdes Geheimnis offenbart und der Arzt nicht dafür Sorge getragen hat, dass der Dienstleister zur Geheimhaltung verpflichtet wurde. Im Kern müssen daher Anwender bzw. Ärzte als Berufsgeheimnisträger die von ihnen beauftragten Dienstleister ggf. zusätzlich in schriftlicher Form zur Verschwiegenheit verpflichten. Anwender sind vor diesem Hintergrund daher gut beraten, den Vertrag zur Auftragsverarbeitung im Hinblick auf die Verschwiegenheitspflicht des Dienstleisters gründlich zu überprüfen.

Drittlandtransfer

→ Bei der Verarbeitung von Daten im Rahmen des Einsatzes von Medizinprodukten kann es teilweise dazu kommen, dass die Daten in Drittländer (= Länder außerhalb der EU/ des EWR) übermittelt werden.
In diesen Fällen muss geprüft werden, in welches Drittland die Daten übermittelt werden und welche Rechtsgrundlage bzgl. der Datenübermittlung für dieses Drittland in Betracht kommt.[12] Insofern besteht zum einen die Möglichkeit, die Datenübermittlung auf einen Angemessenheitsbeschluss nach Art. 45 DS-GVO zu stützen. In diesem Zusammenhang muss stets vorab geprüft werden, ob ein etwaiger Beschluss über ein angemessenes Schutzniveau für das jeweilige Drittland vorliegt. Alternativ können als Rechtsgrundlage auch geeignete Garantien gemäß Art. 45 DS-GVO herangezogen werden, wie etwa der Abschluss von verbindlichen Unternehmensrichtlinien (sog. Binding Corporate Rules) oder von sog. Standardvertragsklauseln. In diesen Fällen ist jedoch darauf zu achten, vorab eine Risikoeinschätzung in Form eines sog. Transfer Impact Assessments (nachfolgend „**TIA**“ genannt) durchzuführen. Darüber hinaus besteht in Einzelfällen für Betroffene auch die Möglichkeit, in die Übermittlung ihrer Daten in ein Drittland gem. Art. 49 Abs. 1 S. 1 lit. a) DS-GVO ausdrücklich einzuwilligen. Ob diese Rechtsgrundlage tatsächlich herangezogen werden kann, sollte im Vorfeld geprüft werden.

→ Aktuelle Entwicklungen in den USA:
Im Hinblick auf die Datenübermittlungen in die USA mussten Anwender bisher stets ein TIA durchführen, da die Datenübermittlung auf die Standardvertragsklauseln gestützt wurde. Seit dem 10. Juli 2023 allerdings können Datenübermittlungen in die USA grundsätzlich auf einen von der EU-Kommission verabschiedeten Angemessenheitsbeschluss gestützt werden. Die jeweiligen Unternehmen mit Sitz in den USA müssen hierfür teilweise noch ein Zertifizierungsverfahren durchlaufen, um sich auf den Angemessenheitsbeschluss berufen zu können. Für Anwender bedeutet dies Folgendes: Sollte eine solche Zertifizierung für das jeweilige US-Unternehmen bereits erfolgt sein, können sich Anwender in Bezug auf die Rechtsgrundlage für die Datenübermittlung nunmehr auf den Angemessenheitsbeschluss berufen, weshalb die Durchführung eines TIAs nicht mehr erforderlich ist. In diesem Zusammenhang sollte jedoch zwingend sichergestellt werden, dass keine Subunternehmer in anderen Drittstaaten eingesetzt werden, da in diesen Fällen nämlich der Angemessenheitsbeschluss allein nicht ausreicht.

[12] https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_4.pdf.

Praxistipp:

Das Bayerische Landesamt für Datenschutzaufsicht hat in Zusammenarbeit mit dem Bayerischen Landesbeauftragten für den Datenschutz eine Handreichung in Bezug auf die Cybersicherheit für medizinische Einrichtungen erstellt, worin einige hilfreiche Praxismaßnahmen überblicksartig in Form einer Checkliste dargestellt sind.[13] Die darin aufgeführten Maßnahmen stellen einen Best-Practice-Ansatz dar, welche einen effektiven Schutz gegen aktuelle Cybersicherheitsbedrohungen unterstützen können und von Anwendern zusätzlich als Hilfestellung für die Anwendung von Medizinprodukten herangezogen werden können.

[13] https://www.lda.bayern.de/media/checkliste/baylda_checkliste_medizin.pdf.

VI. Künstliche Intelligenz und Medizinprodukte

Die Integration künstlicher Intelligenz bei Medizinprodukten hat in den letzten Jahren einen großen Fortschritt gemacht. Es kann mit hoher Wahrscheinlichkeit davon ausgegangen werden, dass die Entwicklung in diesem Bereich in den nächsten Jahren rasant zunehmen wird. Welche rechtlichen Fragestellungen sich in diesem Kontext konkret stellen und worauf Hersteller sowie Anwender achten sollten – insbesondere im Hinblick auf den bevorstehenden „Artificial Intelligence Act“ („AI-Act“) wird in einem gesonderten Whitepaper näher analysiert.

C. Sonderfall: Digitale Gesundheitsanwendungen

Seit Inkrafttreten des Digitale-Versorgungs-Gesetzes (nachfolgend „DVG“ genannt) am 19.12.2019 werden neben den klassischen physischen Medizinprodukten auch sogenannte „Health Apps“ auf dem Markt angeboten, womit eine Zeitenwende für die Gesundheitsbranche geschaffen wurde. Seither können Ärzte und Therapeuten ihren Patienten nunmehr auch digitale Gesundheitsanwendungen (kurz „DiGA“) verschreiben. Im Gegensatz zu den bisherigen gängigen Versorgungsleistungen handelt es sich bei der DiGA also um eine Software oder Anwendung, welche auf digitalen Plattformen wie Smartphones oder Tablets läuft und Ärzte bzw. Therapeuten ihren Patienten – wie bei Medikamenten auch – verschreiben können. Insgesamt also als eine Art verschreibungspflichtiges digitales Medizinprodukt auf Rezept („App auf Rezept“) zu verstehen.

I. Definition

Eine DiGA ist gemäß § 33a SGB V ein Medizinprodukt, welches folgende Eigenschaften hat:

- **Medizinprodukt** der **Risikoklasse I** oder **IIa** (nach MDR oder, im Rahmen der Übergangsvorschriften der MDR, nach MDD).
- Die **Hauptfunktion** der DiGA beruht auf **digitalen Technologien**.
- Die DiGA ist keine digitale Anwendung, die lediglich dem Auslesen oder Steuern eines Gerätes dient; der medizinische Zweck muss wesentlich durch die **digitale Hauptfunktion** erreicht werden.
- Die DiGA unterstützt die **Erkennung**, **Überwachung**, **Behandlung** oder **Linderung von Krankheiten** oder **Linderung von Krankheiten** oder die Erkennung, Behandlung, Linderung oder **Kompensierung** von **Verletzungen** oder **Behinderungen**.
- Die DiGA dient **nicht** der **Primärprävention**.
- Die DiGA wird **vom Patienten oder vom Leistungserbringer und Patienten gemeinsam genutzt**, d. h. Anwendungen, die lediglich vom Arzt zur Behandlung der Patienten eingesetzt werden („Praxisausstattung“), sind keine DiGA.

II. Beispiele

DiGA (+)	DiGA (-)
• Apps für depressive Patienten, welche Informationen zur Erkrankung vermitteln, Stimmungen der Patienten dokumentieren und Anleitungen zu Entspannungsübungen geben. • Apps zur Erinnerung an die Einnahme von Medikamenten, welche ggf. zusätzlich Dosier-vorschläge geben. • Apps für Patienten mit chronisch entzündlicher Darmerkrankung, welche Informationen zur Erkrankung und Ernährung vermitteln, Symptome dokumentieren, Anleitungen zur Erstellung von Ernährungsplänen geben und einen digitalen Einkaufs-begleiter mit Scanfunktion für Lebensmittel bereitstellen.	• Die App dient lediglich als Koordination und Durchführung von Video- / Telefon- / Chatgesprächen zwischen Therapeut und Patient. Weitere therapeutische Leistungen sind nicht umfasst. • Apps für Patienten mit chronisch entzündlicher Darmerkrankung, welche Patienten bei Bedarf mit Ernährungsberatern über eine Chatfunktion oder Telefonate in Kontakt bringen.

1. Aufnahme in das DiGA Verzeichnis

Wer eine DiGA auf den Markt bringen will, muss sich im Vorfeld mit zahlreichen gesetzlichen Vorgaben auseinandersetzen und einige Schritte bei der Umsetzung berücksichtigen: Zunächst müssen Hersteller etwa einen Antrag zur Aufnahme in das „DiGA-Verzeichnis“ stellen.[14] Das Bundesinstitut für Arzneimittel und Medizinprodukte (kurz „**BfArM**“) prüft sodann, ob der Hersteller bei der Entwicklung des Produkts auch sämtliche Anforderungen insbesondere im Hinblick auf Funktionstauglichkeit, Datenschutz und Datensicherheit eingehalten hat. Darüber hinaus müssen Hersteller auch nachweisen, dass das Produkt einen medizinischen Nutzen (z.B. Verbesserung des Gesundheitszustands) oder eine patientenrelevante Struktur- und Verfahrensverbesserung in der Versorgung (z.B. Erkennung oder Linderung von Krankheiten) zur Folge hat.

[14] https://antrag.bfarm.de/de.

2. Datenschutz

Im Hinblick auf den Datenschutz müssen Anwender und Hersteller von DiGA ebenfalls auf die Einhaltung der datenschutzrechtlichen Anforderungen achten. Insoweit gelten für DiGA ebenfalls die oben unter Gliederungspunkt B.IV.1. dargestellten Grundsätze sowie die im DVG dargelegten allgemeinen Anforderungen zum Datenschutz und zur Datensicherheit. Für Hersteller ergeben sich darüber hinaus noch zusätzliche Besonderheiten, die sie berücksichtigen müssen. Insbesondere die Aufnahme in das DiGA-Verzeichnis und die damit verbundene Zulassung der DiGA ist an hohe datenschutzrechtliche Anforderungen geknüpft, welche Hersteller bei der Entwicklung ihres Produkts stets im Auge behalten sollten. Neben der DS-GVO und den bereits unter Gliederungspunkt B.III. skizzierten Vorschriften sind daher zusätzlich die Digitale-Gesundheitsanwendungen-Verordnung (nachfolgend „**DiGAV**“) und die Prüfkriterien BfArM[15] von besonderer Relevanz:

Hierzu zählen insbesondere:

a) DiGAV

→ Von hoher Relevanz sind für Hersteller die in der DiGAV enthaltenen Regelungen. Damit ihr Produkt überhaupt zugelassen wird, müssen Hersteller nämlich insbesondere den in Anlage 1 der DiGAV aufgeführten Fragebogen ausfüllen, welcher in Form von Checklisten abgebildet ist.[16] Die Checklisten gliedern sich in die beiden Themenfelder Datenschutz und Datensicherheit und führen sämtliche relevanten Aspekte, von den datenschutzrechtlichen Grundsätzen bis hin zu Themen wie Zugangskontrollen und Authentisierung, auf. Hersteller müssen im Rahmen dieser Checklisten die Erfüllung der Anforderungen gemäß § 4 DiGAV erklären. Vor diesem Hintergrund stellt § 4 DiGAV ausdrücklich klar, dass aus der digitalen Anwendung heraus und zu Beginn der Nutzung der DiGA eine informierte Einwilligung der betroffenen Person eingeholt werden muss, sofern keine andere Vorschrift die Datenverarbeitung erlaubt.

b) Prüfkriterien

→ Das BfArM hat zudem Prüfkriterien für die Anforderungen an den Datenschutz bei DiGA veröffentlicht. Diese Kriterien werden künftig Grundlage für neue Zertifikate sein, mit denen Hersteller von Gesundheitsanwendungen nachweisen können, dass ihre Anwendungen datenschutzkonform sind. Diese umfassen sowohl die Anforderungen der DS-GVO als auch die erweiterten Anforderungen für DiGA. Der Nachweis der Erfüllung der Anforderungen an den Datenschutz durch den Hersteller ist jedoch erst ab dem 01. August 2024 durch Vorlage eines anhand dieser Prüfkriterien ausgestellten Zertifikates zu führen. Bis zu diesem Zeitpunkt greifen die in § 4 Abs. 6 DiGAV genannten Anforderungen an den Datenschutz.

→ Die Prüfkriterien sind insgesamt in 12 Themenbereiche gegliedert, wobei sie sich an den für die DiGA relevanten Schwerpunkten der DSGVO ausrichten. Für Anwender sind insbesondere die unter Teil 3 des Prüfkriterienkatalogs des BfArM gemachten Ausführungen von Relevanz. Die inhaltlichen Schwerpunkte darin entsprechen im Wesentlichen den oben aufgeführten datenschutzrechtlichen Grundsätzen und formellen Anforderungen.

[15] https://www.bfarm.de/SharedDocs/Downloads/DE/Medizinprodukte/diga-dipa-datenschutzkriterien.pdf?__blob=publicationFile.

[16] https://www.gesetze-im-internet.de/digav/BJNR076800020.html.

D. Checkliste

I. Für Anwender

- ☐ Ist der Prozess im Verarbeitungsverzeichnis dokumentiert?
- ☐ Sofern keine andere gesetzliche Grundlage einschlägig ist:
  Wird zeitlich vor Beginn der Datenverarbeitung eine informierte Einwilligung der betroffenen Person eingeholt?
- ☐ Wurden angemessene technische und organisatorische Maßnahmen ergriffen und umgesetzt?
- ☐ Gibt es einen Notfallplan zum Umgang mit Datenpannen?
- ☐ Werden die betroffenen Personen mithilfe von Datenschutzhinweisen über die Verarbeitung ihrer Daten ausreichend informiert?
- ☐ Wurde vor Einführung des Produkts eine Datenschutz-Folgenabschätzung durchgeführt?
- ☐ Existiert im Hinblick auf die Aufbewahrung der Daten ein Löschkonzept?
- ☐ Sofern Dienstleister eingesetzt werden (bspw. für die Fernwartung): Wurde ein Vertrag zur Auftragsverarbeitung abgeschlossen?
- ☐ Sofern mehrere Verantwortliche die Zwecke und Mittel der Datenverarbeitung bestimmen: Wurde ein Joint Controller Vertrag abgeschlossen?

Im Falle einer Datenübermittlung in ein Drittland:

- ☐ Existiert für die Datenübermittlung eine datenschutzrechtliche Rechtsgrundlage?

II. Für Hersteller

- ☐ Ist sichergestellt, dass die Daten im Rahmen der Datenübertragung verschlüsselt sind?
- ☐ Ist in dem Produkt ein Berechtigungskonzept zwecks Regelung der Zugriffsrechte implementiert?
- ☐ Ist eine Clusterung des Storage-Systems sichergestellt?
- ☐ Ist im Rahmen des Archivformats sichergestellt, dass die Daten auch in Zukunft noch lesbar sind?
- ☐ Ist sichergestellt, dass im Falle einer Fernwartung gegenüber dem Dienstleister keine personenbezogenen Daten offengelegt werden?
- ☐ Können die Daten nach Ablauf einer gewissen Zeit automatisch gelöscht werden?
- ☐ Existieren regelmäßige Updates und Sicherheitspatches für das Medizinprodukt?
- ☐ Gibt es ein Dokument (FAQ Dokument oder ein Whitepaper) mit Datenschutzinformationen für Kunden im Hinblick auf Informationen zu dem Medizinprodukt?
- ☐ Existieren Musterdokumente (bspw. Datenschutz-Folgenabschätzung), welche auf das jeweilige Medizinprodukt abgestimmt sind und den Kunden zur Verfügung gestellt werden?
- ☐ Existiert ein anwenderfreundlicher Vertrag zur Auftragsverarbeitung (Art. 28 DS-GVO) unter Beachtung der einschlägigen rechtlichen Anforderungen (auch zu § 203 StGB), welcher den Kunden zur Verfügung gestellt werden kann?
- ☐ Im Falle von DiGA: Wurden die Vorgaben aus dem Fragenkatalog in Anlage 1 der DiGAV entsprechend umgesetzt?

Unsere Expertinnen und Experten
für Datenschutz beim Einsatz von Medizinprodukten

Fabian Bauer, LL.M.
Senior Associate

+49 69 630001-82
f.bauer@skwschwarz.de

Marius Drabiniok
Associate

+49 69 630001-65
m.drabiniok@skwschwarz.de

Dr. Oliver Hornung
Partner

+49 69 630001-65
o.hornung@skwschwarz.de

Marwah Kamal
Associate

+49 69 630001- 65
m.kamal@skwschwarz.de

Franziska Ladiges, LL.B.
Partnerin

+49 69 630001-29
f.ladiges@skwschwarz.de

10719 Berlin
Kranzler Eck
Kurfürstendamm 21
T +49 30 8892650-0
F +49 30 8892650-10

60598 Frankfurt/Main
Mörfelder Landstraße 117
T +49 69 630001-0
F +49 69 6355-22

20459 Hamburg
Ludwig-Erhard-Straße 1
T +49 40 33401-0
F +49 40 33401-530

80333 München
Wittelsbacherplatz 1
T +49 89 28640-0
F +49 89 28094-32

skwschwarz.de