Der Schutz von Daten, die EU-Datenschutzgrundverordnung

und die (möglichen) Auswirkungen auf MVZ

13.09.2018

Gerald Spyra, LL.M.
RP mbB

spyra@rpmed.de

Vorstellung meiner Person

Gerald Spyra, LL.M.

- **Rechtsanwalt / Partner bei RP**
- **Hohe Affinität für die Informationssicherheit**
- **Spezialisiert auf**
  - **den Informations- / Datenschutz,**
  - **das „Software-Medizinprodukterecht“ und**
  - **die „IT-Forensik“**
- **Externer betrieblicher Datenschutzbeauftragter**

spyra@rpmed.de

Agenda

- **Teil 1:**
- **Immer mehr IT…**

- **Teil 2:**

Der Schutz von Daten = Datenschutz!?

- **Teil 3:**

Datenschutzgrundverordnung – Was ist das und was bedeutet sie für die Praxis?

- **Teil 4:**

Grundprinzipien, Verantwortlichkeiten, Betroffenenrechte, Sanktionen, Datenschutzverstöße

- **Teil 5:**

„Best practice" – Was jetzt zu tun ist?

spyra@rpmed.de

Teil 1

Immer mehr und immer vernetztere IT…

spyra@rpmed.de

Immer mehr, vernetzte IT in MVZ…

- Immer mehr vernetzte IT bzw. „smarte Geräte“ werden in MVZ eingesetzt.
- Nutzer können mit diesen Geräten wie z.B. Smartphones, vermeintlich „sicher“ umgehen, u.a. weil sie diese Geräte auch im PRIVATEN einsetzen!
- Unterschiedlichste Daten können bzw. werden zwischen den Geräten praktisch weltweit (in der „Cloud“) ausgetauscht und sind theoretisch weltweit verfügbar.
- Der Einsatz von vernetzten „smarten Geräten“ verspricht eine erhebliche Qualitätssteigerung und ein erhebliches Kosteneinsparungspotenzial.
- Doch das ist nur die eine Seite der Medaille…

spyra@rpmed.de

Immer mehr IT… Die Konsequenzen

- **Der Gang in die digitale Welt bedeutet, dass wir uns immer mehr in einer „virtuellen", uns fremden Welt bewegen.**
- **Durch den Gang in die virtuelle Welt müssen wir uns ganz neuen, bisher uns unbekannten, „unmenschlichen" Herausforderungen stellen.**
- **Ferner bedeutet dieser Gang, dass „Dritte", die eigentlich nichts mit der Patientenbehandlung zu tun haben, dennoch die Daten rund um die Behandlung des Patienten bekommen können.**
- **Aufgrund des „Gangs" in die virtuelle, digitale Welt müssen wir uns in jedem Fall darüber im Klaren sein, dass die Verarbeitung von Daten immer wichtiger wird…**

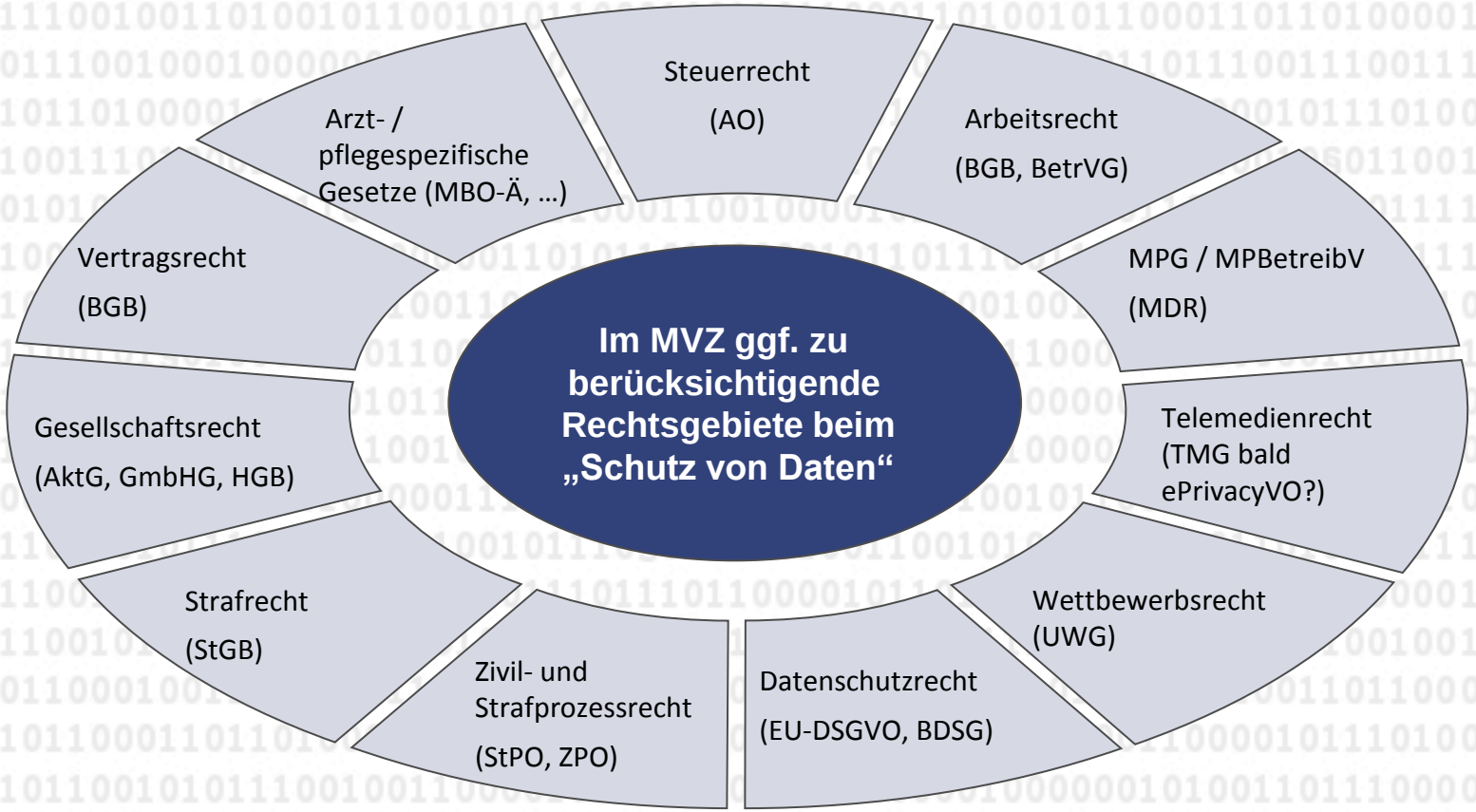
spyra@rpmed.de

Die Bedeutung der Daten und ihrer Verarbeitung

- **Je mehr Prozesse des MVZ mittels vernetzter IT abgebildet werden, umso geschäftskritischer werden diese Prozesse.**
- **Von der ordnungsgemäßen Datenverarbeitung hängt somit immer mehr das „Wohl und Wehe" des Patienten (der jeder von uns sein kann) und natürlich auch das des MVZ ab.**
- **Die Gewährleistung eines ausreichenden „Schutz von Daten" wird aufgrund der Geschäftskritikalität immer mehr zu einem bedeutenden „Compliance- Thema" für ein MVZ.**
- **Und diesbezüglich existiert ein wahrer Gesetzesdschungel…**

spyra@rpmed.de

Einblick in den “Gesetzesdschungel” im Bereich “Schutz von Daten” bei einem MVZ



- **Und gerade deshalb sollte man den „Schutz von Daten“ nicht auf die leichte Schulter nehmen…**

Teil 2

Der Schutz von Daten
=
Datenschutz?

spyra@rpmed.de

Alles Datenschutz oder was?

- **Eines schon vorweg….**

„Der „Schutz von Daten"
ist nicht gleich „Datenschutz".

- **Daten gilt es nämlich aus unterschiedlichen (Rechts-) Gründen zu schützen.**

spyra@rpmed.de

Wieso sollte man Daten schützen?

- **Der Schutz eines Datums bzw. von Daten, kann aus unterschiedlichen Rechtsgründen notwendig sein wie z. B.:**
  - **Zum Schutz der Privatsphäre („Freiheit"),**
  - **zum Schutz des Unternehmens,**
  - **zum Schutz der „Nachweisbarkeit",**
  - **zum Schutz des „Vertrauens",**
  - **zum Schutz der Gesundheit und des Lebens,**
  - **…**
- **Frage: Wieso können eigentlich für ein und dasselbe „Datum" unterschiedliche Schutzgründe einschlägig sein?**
- **Antwort: Weil es m.A. nach primär nicht um Daten, sondern um Informationen geht!**

spyra@rpmed.de

„Daten“ vs. „Informationen“

- **Man sollte es tunlichst vermeiden, die Begriffe „Daten“ und „Informationen“ gleichzusetzen.**
- **Daten sind nämlich nur der „Rohstoff“, der für sich gesehen eigentlich keinen großen Wert hat (ähnlich wie ein Rohdiamant)!**
- **Wertvoll machen ein Datum erst:**
  - **die Informationen (das „Wissen“),**
  - **die aus ihm**
  - **mittels entsprechender „Intelligenz“ (Algorithmen) gewonnen werden können.**

spyra@rpmed.de

Das Problem „Daten“

- **Ein einziges Datum kann Millionen unterschiedlicher Informationen beinhalten.**
- **Das Problem ist jedoch, dass ein Datum seine Informationen oftmals nicht (alle) sofort preisgibt.**
- **Hierzu ein Beispiel:**

Welche Information enthält die Zahlenfolge „1 4 9 2“ ???

spyra@rpmed.de

„1 4 9 2“

- **Für sich betrachtet, steht diese Zeilenfolge isoliert dar und sagt erst einmal wenig aus.**
- **Es könnte sich um das Jahr der Entdeckung von Amerika durch Kolumbus handeln….**
- **Daher kann man jedem diese Zahlenfolge mitteilen, oder?**
- **Und wenn es der PIN-Code zu einem bestimmten Konto oder eine spezielle Medikamentendosis für einen bestimmten Patienten ist…?**
- **Merke: Je nach Kontext, in den ein Datum gebracht werden kann, kann die Bedeutung eines Datums schnell von „unbedeutend“ in „sehr bedeutend“ wechseln.**

spyra@rpmed.de

„Auf einen Blick“

- **Daten sind das Roh-Öl bzw. die Roh-Diamanten des 21. Jahrhunderts!**
- **Wir wissen oftmals nicht (und können es auch nicht abschätzen), welche Informationen ein einziges Datum für sich beinhalten kann!**
- **Daher sollten wir mit Daten grundsätzlich sensibel umgehen…**
- **Und das zeigt uns auch das „Datenschutzrecht“….**

spyra@rpmed.de

Das Datenschutzrecht

- **Das Datenschutzrecht erfasst „nur" personenbezogene Daten (Informationen) des Betroffenen.**
- **Patientendaten sind zumeist „Gesundheitsdaten" (besondere Arten von personenbezogenen Daten).**
- **Die Erhebung, Verarbeitung oder Nutzung dieser Daten ist aufgrund ihrer Sensibilität nur unter strengen Voraussetzungen möglich (wie beim „Geheimnis").**
- **Daher sollten wir uns nun, mit dem bald für ganz Europa geltenden Datenschutzrecht, der EU-Datenschutzgrundverordnung beschäftigen…**

spyra@rpmed.de

Teil 3

Datenschutzgrundverordnung – Was ist die DSGVO und was bedeutet sie für die Praxis?

spyra@rpmed.de

Datenschutz in Europa (1)

- Der Datenschutz in Europa, war seit jeher ein wichtiges Thema…
- Da unterschiedliche Datenschutzniveaus Handelshindernisse darstellen können, gab es bereits erste Ansätze eines europäischen Datenschutzrechts im Jahre 1995 mit der Schaffung der sog. EU-Datenschutzrichtlinie.
- Diese musste zunächst von jedem EU-Mitgliedsstaat in nationales Recht umgesetzt werden.
- Die Regelungen der Richtlinie beinhalteten einen nicht unerheblichen Gestaltungsspielraum für die nationalen Gesetzgeber, was wiederum nicht ohne Konsequenzen blieb…

spyra@rpmed.de

Datenschutz in Europa (2)

- **Durch die „Spielräume“ kam es schnell zu unterschiedlich hohen Datenschutzniveaus in den jeweiligen EU-Mitgliedstaaten.**
- **Diese unterschiedlichen Datenschutzniveaus waren u.a. ein Faktor für Standortentscheidungen (Irland).**
- **Aufgrund unterschiedlichen Datenschutzniveaus, kam es u.a. zu (Daten-) Handelshindernissen, die es ja aber eigentlich unbedingt zu vermeiden galt…**
- **Kurz: Die EU-Datenschutzrichtlinie hat versagt und der EU-Gesetzgeber musste es richten (oder auch nicht)!**
- **Dieses versucht er nun mit der DSGVO…**

spyra@rpmed.de

Datenschutz in Europa (3)

- **Die DSGVO gilt in ganz Europa ab dem 25. Mai 2018 direkt (braucht grundsätzlich nicht mehr in nationales Recht umgesetzt werden).**
- **Sie verdrängt (in ihrem Anwendungsbereich) das bisher geltende nationale Datenschutzrecht.**
- **Nur da, wo der nationale Gesetzgeber in der DSGVO ermächtigt wird, eigene Regelungen zu schaffen, finden diese zusätzlich zur DSGVO Anwendung (z. B. BDSG-Neu).**
- **Und was sind nun die Ziele der DSGVO? …**

spyra@rpmed.de

Ziele der VO

- **Die Zielvorgaben der EU-DSGVO sind durch Erwägungsgrund 13 klar formuliert.**

- **Die VO soll in ganz Europa**
  - **ein einheitliches Datenschutzniveau schaffen,**
  - **datenschutzrechtliche Unterschiede beseitigen und**
  - **dadurch die notwendige Rechtssicherheit und Transparenz für Datenverarbeitungen in ganz Europa schaffen.**

- **Kinder sollen dabei besonders geschützt werden.**

- **Und weil die DSGVO Auswirkungen auf all unsere Lebensbereiche hat, sollte man sich mit dieser (R)Evolution des Datenschutzes näher auseinandersetzen.**

spyra@rpmed.de

Teil 4

Grundprinzipien;
Verantwortlichkeiten;
Betroffen- / Patientenrechte;
Sicherheit;
Sanktionen
…

spyra@rpmed.de

Grundprinzipien der Verarbeitung - Art. 5

- **In der VO sind Grundprinzipien festgelegt, die für GRUNDSÄTZLICH (Ausnahmen bestätigen die Regel) jede Verarbeitung gelten.**

- **Jede Datenverarbeitung in einem MVZ muss sich an diesen orientieren…**

- **Es handelt sich um die Grundsätze:**
  - **der Rechtmäßigkeit, der Verarbeitung nach Treu und Glauben und der Transparenz;**
  - **der Zweckbindung;**
  - **der Datenminimierung;**
  - **der Richtigkeit;**
  - **der Speicherbegrenzung;**
  - **der Integrität und der Vertraulichkeit (der Sicherheit);**
  - **der Rechenschaftspflicht.**

spyra@rpmed.de

Rechtmäßigkeit, Treu und Glauben, Transparenz (Art. 5 Abs. 1 lit a)

- **Nach der VO müssen pbD:**
- ***„auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden"***

- **Mithin muss jede Datenverarbeitung entsprechend der rechtlichen Vorgaben (Rechtmäßigkeit),**

- **dem Verhalten eines „redlichen und anständigen" Menschen entsprechen und fair sein (Treu und Glauben).**

- **Und all dieses muss für den Betroffenen nachvollziehbar sein, bzw. er muss die Möglichkeit haben, von den jeweiligen Umständen zu erfahren (Transparenz).**

- **Zunächst zur Rechtmäßigkeit…**

spyra@rpmed.de

Rechtmäßigkeit (Art. 5 Abs. 1 lit a)

- **Der Grundsatz der Rechtmäßigkeit besagt, dass jede Datenverarbeitung einer gesetzlichen Grundlage bedarf.**
- **Die beiden maßgeblichen gesetzlichen Rechtmäßigkeitsvorschriften der DSGVO befinden sich in:**
  - **Art. 6 (für „normale" personenbezogene Daten) und**
  - **Art. 9 (für „besondere")**
- **Diese Vorschriften beinhalten Regelungen, die festlegen, unter welchen Voraussetzungen (zu welchen Zwecken) eine Datenverarbeitung zulässig sein kann.**
- **Im jeweiligen Einzelfall gilt es für die Rechtmäßigkeit weitere Anforderungen zu beachten (Art. 26, 28 usw.)**
- **Und immer gilt es die „Fairness" zu beachten…**

spyra@rpmed.de

Treu und Glauben (Fairness) (Art. 5 Abs. 1 lit a)

- **Der Begriff „Treu und Glauben" ist die (m.A. nach misslungene) Übersetzung des englischen Begriffs „Fairness".**
- **Eine Datenverarbeitung muss daher immer „fair" sein.**
- **Mithin darf sie für einen Betroffenen keine „Überraschungen" beinhalten (unerlaubte Datenübermittlungen usw.) und es muss ihm die Geltendmachung seiner Rechte ermöglicht werden.**
- **Zur Auslegung des Gebots der „Fairness" lassen sich Analogien zu den AGB-Regelungen des BGB ziehen.**
- **Das Gebot der „Fairness" ist daher auch eng mit dem Gebot der „Transparenz" gekoppelt.**

spyra@rpmed.de

Transparenz (Art. 5 Abs. 1 lit a)

- **Der in der DSGVO enthaltene Transparenzgrundsatz bezieht sich grundsätzlich nur darauf, dass ein Betroffener nachvollziehen bzw. erfahren können muss, was bei der Datenverarbeitung geschieht.**
- **Damit ein Verantwortlicher jedoch dem Betroffenen Transparenz verschaffen kann, muss er selber erst einmal durchblicken (bei sich selber Transparenz schaffen).**
- **Mithin ist der Grundsatz der Transparenz eine der essenziellen Säulen des Datenschutzes.**
- **Denn wenn ein entsprechender Durchblick besteht, lässt sich auch nachprüfen, ob die Zweckbindung beachtet wurde…**

spyra@rpmed.de

Zweckbindung (2)

- **Schon bei Erhebung der Daten, müssen die Zwecke eindeutig festgelegt sein und die Verarbeitung muss einem legitimen Zweck dienen!**
- **Eine (Weiter-) Verarbeitung zu anderen Zwecken ist nicht gestattet, wenn die Zwecke nicht miteinander vereinbar (kompatibel) sind.**
- **Die Weiterverarbeitung (Zweckänderung) für öffentliche Zwecke (Archiv-, wissenschaftlich- / historisch oder statistische Zwecke) ist privilegiert und es wird vermutet, dass sie als vereinbar mit ursprünglichen Zwecken gilt.**
- **Eine Ausprägung der Zweckbindung ist auch das Gebot der „Datenminimierung"...**

spyra@rpmed.de

Datenminimierung (Art. 5 Abs. 1 lit. c)

- **Nach der VO muss eine Verarbeitung pbD ferner immer „dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein."**
- **Das kennen wir in Deutschland als „Datenvermeidung" und „Datensparsamkeit".**
- **Es gilt deshalb auch nach der VO: „Am besten keine pbD verarbeiten und wenn doch, dann bitte immer nur so viel wie nötig, um den Zweck zu erreichen!!!"**
- **Und natürlich muss auch immer gewährleistet sein, dass die Daten „richtig" und „aktuell" sind…**

spyra@rpmed.de

Richtigkeit (Art. 5 Abs. 1 lit. d)

- **PbD müssen der VO nach *„sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.“***
- **Ein Verantwortlicher muss deshalb gewährleisten und prüfen, dass Daten stets auf dem neuesten Stand und richtig sind!**
- **Sind sie es nicht, muss er diese UNVERZÜGLICH löschen oder berichtigen.**
- **Und außerdem darf er die pbD nicht „unbegrenzt“ lange speichern…**

spyra@rpmed.de

Speicherbegrenzung (Art. 5 Abs. 1 lit. e)

- **Daten sind immer nur so lange speichern, wie man sie für einen oder mehrere bestimmte Zwecke braucht (Big Data adieu).**
- **Sind sie nicht mehr für die Erfüllung der Zwecke notwendig, müssen sie folglich „gelöscht" werden.**
- **Sie dürfen länger aufbewahrt werden zu Archivierungs-, Wissenschafts- oder Forschungszwecken oder statistischen Zwecken, wenn diese konform mit der VO sind (Art. 89) und der Verantwortliche die entsprechend erforderlichen TOM getroffen hat..**
- **Die erforderlichen TOM sind insbesondere auch notwendig, um die Integrität und die Vertraulichkeit der pbD zu gewährleisten.**

spyra@rpmed.de

Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f) - „Datensicherheit“

- **Bei der Verarbeitung von Daten ist immer die erforderliche „Sicherheit“ (entsprechend des RISIKOS!!! der Datenverarbeitung) zu gewährleisten.**
- **Daher muss ein MVZ sicherstellen, dass stets immer die Vertraulichkeit, die Integrität und die Verfügbarkeit (C I A) mittels risikoadäquaten Maßnahmen eingehalten wird!**
- **Daher sind immer wieder Anpassungen an den technischen und organisatorischen Schutzmaßnahmen notwendig, besonders wenn man immer „modernere / smarte IT“ einsetzen will (es gilt immer den aktuellen Stand der Technik zu halten).**
- **Und für die Einhaltung von all dem vorher Gesagten ist der Verantwortliche „verantwortlich“…**

spyra@rpmed.de

Rechenschaftspflicht / Beweislast (Art. 5 Abs. 2)

- **Nach Art. 5 Abs. 2 ist der „Verantwortliche für die Einhaltung (der Anforderungen) des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können.**

- **Aus diesem Grundsatz resultiert eine (gerichtliche) Beweislast.**

- **Ein Verantwortlicher muss deshalb beweisen können, dass er alles richtig gemacht hat (was nicht dokumentiert ist, ist auch nicht geschehen).**

- **Nur wenn man entsprechend dokumentiert, kann man als Verantwortlicher die Rechtmäßigkeit der Verarbeitung (Art. 6 und Art. 9) auch nachweisen…**

spyra@rpmed.de

Der Verantwortliche

- **Der „Verantwortliche“ wird definiert als: *die***
  - ***natürliche* oder *juristische Person*,**
  ***Behörde*, *Einrichtung* oder *andere Stelle*,**
  ***die allein* oder *gemeinsam* mit anderen**
  über die Zwecke und Mittel der Verarbeitung von
  ***personenbezogenen Daten entscheidet*;**

- **Von der Verantwortlichkeit leiten sich alle zu erfüllenden Pflichten ab!**

- **Entscheidend ist es deshalb im EINZELSACHVERHALT zu bestimmen, wer über die Mittel und Zwecke der Datenverarbeitung entscheidet (bei „Cloud und Co.“ kein einfaches Unterfangen).**

spyra@rpmed.de

Das MVZ als Verantwortlicher

- **Ein MVZ dürfte in den meisten Fällen Verantwortlicher für die Datenverarbeitung sein – hängt aber auch sehr von der konkreten rechtlichen / tatsächlichen Ausgestaltung ab.**
- **Ihm obliegt die Einhaltung der gesamten datenschutzrechtlichen Anforderungen – Berufsrechtlich gilt es dieses im Einzelfall zu klären!**
- **Damit obliegt ihm gleichzeitig auch die Nachweisführung über die Ordnungsgemäßheit (Rechenschaftspflicht).**
- **Das MVZ ist nicht zuletzt auch dasjenige, an das sich Betroffene, Aufsichtsbehörden usw. primär wenden.**
- **Es gilt zu prüfen, ob das MVZ mit anderen „gemeinsame Verantwortliche" sein können.**

spyra@rpmed.de

Gemeinsame Verantwortliche (Art. 26)

- **Hierbei handelt es sich um eine für Deutschland „neue" Rechtsfigur.**
- **Nach der VO ist es explizit möglich, dass sich zwei oder mehr Verantwortliche für die Datenverarbeitung verantwortlich zeichnen und gemeinsamen über die Mittel und Zwecke der Datenverarbeitung entscheiden.**
- **Dieses muss in einer Vereinbarung in transparenter Form erfolgen, und klar definieren, wer, für was (welchen Bereich), wie, usw. verantwortlich ist.**
- **Ein Betroffener kann seine Rechte grds. gegenüber allen Verantwortlichen, gleich geltend machen!**
- **Und ist so etwas auch bei einem MVZ denkbar?**

spyra@rpmed.de

Gemeinsame Verantwortliche bei einer gemeinsamen Zusammenarbeit

- **Es ist durchaus denkbar, dass ein MVZ mit anderen Praxen, Kliniken, Forschungsinstitutionen gemeinsam Datenverarbeitungen durchführt.**
- **Gerade wenn sie gemeinsame „Portale" etc. nutzen, gilt es die Verantwortlichkeiten genau zu beleuchten.**
- **Insofern sollte man prüfen, ob man eine gemeinsame Verantwortlichkeit vereinbart und in einem Vertrag / Vereinbarung entsprechend regelt**
- **Ganz besonders wichtig ist dabei die Identifikation der gemeinsamen Verarbeitungen und der Verarbeitungszwecke.**
- **Wenn eine Partei jedoch streng weisungsgebunden gegenüber einer anderen die Daten verarbeiten soll, kann sie auch Auftragsverarbeiter sein…**

spyra@rpmed.de

Auftrags(daten)verarbeiter (Art. 4 Nr. 8)

- **Auftragsverarbeiter ist nach der VO eine *„natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;“***

- **Wie bisher, ist es beim Auftragsverarbeiter essenziell, dass er ggü. dem Verantwortlichen weisungsgebunden ist.**

- **Entscheidet ein Auftragsverarbeiter (eigenmächtig) über die Mittel und Zwecke der Datenverarbeitung, wird er zum Verantwortlichen (Art. 28 Abs. 10)!!**

- **Aufgrund der oftmals schwierigen Abgrenzung zum gemeinsamen Verantwortlichen ist es für ein MVZ essenziell wichtig, seine Auftragsverarbeiter genau zu identifizieren…**

spyra@rpmed.de

Auftragsverarbeiter eines MVZ

- **Weil immer mehr Leistungen outgesourced werden, muss geprüft werden, ob diese Externen die Daten wirklich im Auftrag verarbeiten (sollen) – umfassende Vertragsprüfung.**
- **Typische Beispiele einer Auftragsverarbeitung sind:**
  - **der Einsatz von IT-Dienstleistern;**
  - **Unternehmen, die Daten vernichten sollen;**
  - **Hersteller von Medizin- / Softwareprodukten, die sich zu Wartungszwecken aufschalten;**
  - **…**
- **Mit diesen Unternehmen gilt es ganz besondere, auf den jeweiligen Einzelfall zugeschnittene Verträge zu schließen.**
- **Die Auftragsverarbeitung ist wiederum von der Datenübermittlung an einen weiteren Verantwortlichen zu unterscheiden…**

spyra@rpmed.de

Datenübermittlung an einen anderen Verantwortlichen

- **Die Auftragsverarbeitung ist streng von der Datenübermittlung an einen weiteren Verantwortlichen (ehemals Funktionsübertragung) zu unterscheiden.**

- **Bei einer solchen Verarbeitung soll derjenige, der die Daten erhält, diese in eigener Verantwortlichkeit, aufgrund seiner Fachkunde verarbeiten.**

- **Im Unterschied zur Auftragsverarbeitung fehlt es daher an einer strengen Weisungsgebundenheit.**

- **Und gibt es auch solche Übermittlungen bei einem MVZ…?**

spyra@rpmed.de

Datenübermittlung an einen anderen Verantwortlichen

- **Datenübermittlungen an einen weiteren Verantwortlichen dürften bei einem MVZ sogar häufiger vorliegen als eine Auftragsverarbeitung.**

- **Beispiele:**
  - **Übermittlung von Daten an ein Labor,**
  - **Übermittlung von Daten an ein Medizinprodukteunternehmen, das aufgrund der Daten entsprechende Medizinprodukte maßgeschneidert anfertigt,**
  - **Datenübermittlungen an Finanzamt, Steuerberater, Rechtsanwälte usw.**

- **Die Verantwortlichen sind für die jeweilige Datenverarbeitung verantwortlich und müssen auch die Betroffenenrechte erfüllen...**

spyra@rpmed.de

„Sind wir jetzt nicht alle ein bisschen betroffen?“

spyra@rpmed.de

Was ändert sich mit der DSGVO hinsichtlich der Betroffenenrechte?

Das sagt uns Erwägungsgrund 11 der DSGVO:

„Ein unionsweiter wirksamer Schutz personenbezogener Daten erfordert die Stärkung und präzise Festlegung der Rechte der betroffenen Personen sowie eine Verschärfung der Verpflichtungen für diejenigen, die personenbezogene Daten verarbeiten und darüber entscheiden,…"

spyra@rpmed.de

Der „Betroffene“

- **Die Rechte des Betroffenen wurden durch die EU-DSGVO (insbesondere in Kapitel III) gestärkt…**
- **Das wiederum hat erhebliche Auswirkungen auf die Pflichten des Verantwortlichen.**
- **Aus der Stärkung der Rechte des Betroffenen, erwachsen gleichzeitig verstärkte Verpflichtungen des Verantwortlichen.**
- **Er muss diese Pflichten insbesondere bei seinen Prozessen / Workflows berücksichtigen (PDCA).**
- **Der Verantwortliche sollte sich daher intensiv mit den unterschiedlichen Arten von Betroffenenrechten der DSGVO auseinandersetzen.**

spyra@rpmed.de

Die Arten von Betroffenenrechten

- **In der DSGVO lässt sich zwischen unterschiedlichen Arten von Betroffenenrechten unterscheiden, nämlich Rechte,**
  - **durch die der Betroffene eine Verarbeitung gestatten kann;**
  - **durch die sich der Betroffene informieren kann bzw. er informiert werden muss;**
  - **durch die der Betroffene einschreiten kann;**
  - **durch die sich der Betroffene „Hilfe holen" kann;**
  - **durch die der Betroffene einen etwaig erlittenen Schaden geltend machen bzw. kompensieren kann.**

- **Die Ausübung dieser Rechte durch die Betroffenen ist erst dann möglich, wenn der Verantwortliche entsprechende Transparenz geschaffen hat...**

spyra@rpmed.de

Transparenz und Modalitäten
Art. 12 - Los geht's…

- **Die Transparenzpflicht ist eine Konkretisierung des Transparenzprinzips in Art. 5 Abs. 1 lit. a) DSGVO.**

- **Der Verantwortliche muss geeignete Maßnahmen treffen, um dem Betroffenen alle Informationen gemäß:**
  - **Artt. 13 und 14 (Informationspflichten bei der Verarbeitung) und**
  - **alle Mitteilungen gemäß Artt. 15 bis 22 (Auskunftspflichten bei Widerruf, Löschung, etc.),**

in

- **präziser,**
- **transparenter,**
- **verständlicher und**
- **leicht zugänglicher Form in**
- **einer klaren und**
- **einfachen Sprache zu vermitteln…**

- **Und wie soll man es machen?**

spyra@rpmed.de

Transparenz und Modalitäten
Art. 12 - Weiter geht's

- **Das Erteilen dieser Informationen erfolgt**
  - **grds. schriftlich oder in anderer Form,**
  - **gegebenenfalls auch elektronisch.**

- **Im Einzelfall kann die Info auch mündlich erteilt werden, wenn Betroffener es verlangt und dieser seine Identität nachgewiesen hat.**

- **Der Verantwortliche muss dem Betroffenen die Ausübung seiner Rechte (Artt. 15 bis 22) erleichtern (wie auch immer das geschehen soll).**

- **Die Transparenzpflicht ist eine Grundvoraussetzung, damit der Betroffene die Datenverarbeitung „gestatten" kann...**

spyra@rpmed.de

Die „Gestattung“ durch den Betroffenen

- **Der Betroffene kann als „Eigentümer“ der Daten praktisch alle Datenverarbeitungshandlungen der Verantwortlichen legitimieren.**

- **Dieses geschieht durch seine Zustimmung bzw. seine Einwilligung.**

- **Auch wenn früher häufig versucht wurde, mittels Einwilligungen die Datenverarbeitung zu legitimieren, dürfte dieses heute nicht mehr so einfach möglich sein.**

- **Um das Wesen der Einwilligung zu ergründen gilt es, sich zunächst den Begriff der Einwilligung vor Augen zu führen…**

spyra@rpmed.de

Begriff der Einwilligung

- **Eine Einwilligung muss Art. 4 Nr. 11 DSGVO folgend:**
  - **freiwillig (ohne ausgeübten oder empfundenen Zwang)**
  - **für einen konkreten / bestimmten Fall**
  - **informiert (umfassende Kenntnis der Sachlage und Risiken)**
  - **unmissverständlich (klar und deutlich) sein.**

- **Sie kann ausdrücklich (Opt-IN) oder konkludent erfolgen.**

- **Aufgrund des Machtungleichgewichts zwischen Arzt und Patient, dürften Einwilligungen von Patienten (sie wollen ja behandelt werden) gegenüber Ärzten oftmals nicht wirklich freiwillig erfolgen!!!**

- **Die Anforderungen zur Einwilligung kommen aus Art. 7…**

spyra@rpmed.de

Art. 7 kompakt

- **Falls eine Einwilligung erteilt wurde, muss der Verantwortliche diese immer nachweisen können (Rechenschaftspflicht → Dokumentation)!**
- **Das Ersuchen der Einwilligung muss in klarer und einfachen Sprache erfolgen (bei anderen Sachverhalte klar darstellen, wodrauf sich Einwilligung bezieht).**
- **Es gilt eine jederzeitige Widerrufsmöglichkeit vorzusehen („ex nunc" Wirkung) und darauf hinzuweisen (inkl. Folgen).**
- **Kopplungsverbot der Einwilligung (Problem bei Freiwilligkeit, wenn Leistung von Einwilligung abhängig gemacht wird).**
- **Und ganz spannend ist es bei „alten Einwilligungen"…**

spyra@rpmed.de

Was machen wir mit alten Einwilligungen?

- **Es gilt der Grundsatz, dass bestehende Einwilligungen unwirksam werden, wenn sie nicht die Anforderungen der DSGVO erfüllen.**
- **Nur die Einwilligungen, die sowohl die Anforderungen der EU-Datenschutzrichtlinie als auch die der DSGVO abbilden, behalten mit Geltung der DSGVO ihre Wirksamkeit.**
- **Daher sollten alte Einwilligungserklärungen hinsichtlich ihrer Vereinbarkeit mit den Anforderungen der DSGVO überprüft und ggf. angepasst werden.**
- **Gerade bei einer Einwilligung gilt es, damit der Betroffene wirksam einwilligen kann, ihn ausreichend zu informieren…**

spyra@rpmed.de

Die „Informationsrechte“ des Betroffenen bzw. Pflichten des Verantwortlichen

- **Die in der DSGVO enthaltenen Informationsrechte bzw. -pflichten sind:**
  - **Informationspflichten bei Direkterhebung (Art. 13)**
  - **Informationspflichten bei Dritterhebung (Art. 14)**
  - **Auskunftsanspruch des Betroffenen (Art. 15)**
  - **Mitteilungspflicht bei Berichtigung (Art. 19)**
  - **Recht auf Datenübertragbarkeit (Art. 20)**
  - **Informationspflichten bei Datenpannen (Art. 33, 34) (gehe ich bei der „Sicherheit“ drauf ein).**

- **Und dann gibt es ja auch noch die Eingriffsrechte von Betroffenen…**

spyra@rpmed.de

Die „Eingriffsrechte“ des Betroffenen

- **Die Eingriffsrechte des Betroffenen sind:**
  - **Widerrufsrecht(e) (besonders bei einer Einwilligung gem. Art. 7 Abs. 3);**
  - **Berichtigung (Art. 16);**
  - **Löschungsanspruch / Recht auf Vergessenwerden (Art. 17);**
  - **Einschränkung der Verarbeitung (Sperrung) Art. 18;**
  - **Widerspruchsrecht beim Direktmarketing oder der Forschung Art. 21).**

- **Und dann hat der Betroffene auch immer die Möglichkeit, sich „Hilfe zu holen“...**

spyra@rpmed.de

Die „Hilfeholrechte“ des Betroffenen (Zusammenfassung)

- **Recht den Datenschutzbeauftragten zu konsultieren (Art. 38 Abs. 4).**
- **Recht, sich bei einer Aufsichtsbehörde zu beschweren (Art. 77 Abs. 1) – inkl. Recht der gerichtlichen Beschwerde bei Untätigkeit der Aufsichtsbehörde.**
- **Recht des Betroffenen Verbände usw. mit der Durchsetzung der Rechte zu beauftragen (Art. 80 DSGVO, UklaG (Wettbewerbsrecht).**
- **Wenn man das Datenschutzrecht und die Rechte des Betroffenen nicht ernst nimmt, drohen mannigfaltige Sanktionsmöglichkeiten...**

spyra@rpmed.de

Die Sanktionsmöglichkeiten bei Verstößen

- **Die DSGVO und die anderen Gesetze im Bereich Schutz von Daten halten einen „bunten Strauß" an Sanktionsmöglichkeiten bereit, die bei Verstößen drohen, wie:**
  - **Bußgelder (kleine & große), die von der Aufsichtsbehörde verhängt werden können;**
  - **Weitere Maßnahmen der Aufsichtsbehörde**
  - **Entzug der Zulassung / Untersagen der Berufsausübung**
  - **Geld- bzw. Freiheitsstrafen,**
  - **Schadensersatzansprüche (materielle und immaterielle Schäden)**
  - **Abmahnungen z. B. von Verbraucherzentralen oder Mitbewerbern (Datenschutz als Marktverhaltensregel);**
  - **…**
- **Um daher sollte man schauen, dass alles „sicher" ist…**

spyra@rpmed.de

Die „Sicherheit“

Alles „sicher“ oder was?

spyra@rpmed.de

Art. 24 - Verantwortung des für die Verarbeitung Verantwortlichen (1)

- **Art. 24 stellt die Generalklausel / den Programmsatz für den Verantwortlichen dar und sagt bemerkenswert klar, was der Verantwortliche grundsätzlich so alles zu tun hat.**

- **So heißt es:**

„Der Verantwortliche setzt unter Berücksichtigung

- ***der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie***
- ***der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen***
- ***geeignete technische und organisatorische Maßnahmen um,***
- ***um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt.“***

- ***„Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.“***

- **Daraus lässt sich schon so einiges erkennen / ableiten…**

spyra@rpmed.de

Art. 24 - „kompakt“

- **Im Prinzip legt Art. 24 dem Verantwortlichen (und in Konsequenz auch dem Auftragsverarbeiter) eine Pflicht zur Durchführung von RISIKOMANAGEMENT auf…**
- **Ein Verantwortlicher muss jeweils ermitteln, welche Daten er, in welchem Umfang, zu welchen Zwecken, wie verarbeitet und welche weiteren Umstände dieser Verarbeitung zugrunde liegen.**
- **Entsprechend der Eintrittswahrscheinlichkeit und der Schwere der Schäden, muss er das Risiko der Datenverarbeitungen „bewerten“ und entsprechende technische und organisatorische Maßnahmen ergreifen…**
- **Das alles muss er entsprechend nachweisen können.**
- **Und daher ist die Gewährleistung von „Sicherheit“ alles andere als ein einfaches Unterfangen…**

spyra@rpmed.de

Art. 32 - Sicherheit der Verarbeitung - Vorbemerkung

- **Die VO sieht, anders als viele deutsche Gesetze - keinen Katalog / keine Checkliste wie z. B. in Anlage zu § 9 BDSG, mehr vor.**

- **Vielmehr dürfte es nun auf die Gesamtschau bzw. die Effektivität / Effizienz der jeweils getroffenen TOM ankommen.**

- **Somit muss man nun selber „kreativ" werden und einen Weg finden, wie (nach welchen Kriterien) man die getroffenen Maßnahmen strukturiert, dokumentiert und ggf. „präsentiert".**

- **Möglicherweise empfiehlt sich diesbezüglich eine ähnliche Vorgehensweise / Kategorisierung wie bei der ISO 2700XX.**

spyra@rpmed.de

Art. 32 - Sicherheit der Verarbeitung (Risikomanagement)

- **Art. 32 ist die Konsequenz aus dem den Verantwortlichen / Auftragsverarbeiter obliegenden Risikomanagements.**

- **So müssen sie unter Berücksichtigung:**
  - **des Stands der Technik,**
  - **der Implementierungskosten und**
  - **der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung**

sowie

  - **der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen**
  - **geeignete technische und organisatorische Maßnahmen treffen,**
  - **um ein dem Risiko angemessenes Schutzniveau zu gewährleisten;**

spyra@rpmed.de

Art. 32 - Sicherheit der Verarbeitung (Maßnahmen)

- **Art. 32 zählt (nicht abschließend) einige Maßnahmen auf, die getroffen bzw. bei jeder Verarbeitung evaluiert werden sollten.**

- **So zählen hierzu bspw.:**
  - **die Pseudonymisierung und die Verschlüsselung;**
  - **die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;**
  - **die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen (Recovery);**
  - **ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM.**

spyra@rpmed.de

Art. 32 - Beurteilung des Schutzniveaus / Sicherstellung Weisungsgebundenheit

- **Ob ein angemessenes Schutzniveau vorliegt, muss im Einzelfall bewertet werden und dabei sind müssen insbesondere:**
  - **die Risiken berücksichtigt werden, die bei der Verarbeitung durch (unbeabsichtigte, unrechtmäßige) Vernichtung, Verlust, Veränderung oder Offenbarung drohen.**

- **Faktoren zum Nachweis der angemessenen Maßnahmen können bspw.:**
  - **genehmigte Verhaltensregeln (Art. 40) oder**
  - **genehmigte Zertifizierungsverfahren (Art. 42)**

  sein.

- **Wenn keine ausreichende Sicherheit gegeben ist und es zu Datenschutzverletzungen kommt, sind diese meldepflichtig…**

spyra@rpmed.de

Art. 33 – Meldung bei Datenschutzverletzungen

- **Wenn Daten des MVZ von Personen / Organisationen zur Kenntnis genommen werden können, die auf diese eigentlich nicht zugreifen dürften, liegt schon eine Datenschutzverletzung vor (mindestens die „Vertraulichkeit“ ist verletzt).**
- **Diese Verletzung ist der Aufsichtsbehörde grundsätzlich binnen 72 Stunden nach Bemerken zu melden.**
- **Erfolgt diese Meldung nicht in der entsprechenden Zeit, ist dieser Verstoß „bußgeldbewährt“ („kleines“ Bußgeld).**
- **Daher gilt es unbedingt, einen entsprechenden „Meldeprozess“ inkl. Risikomanagement zu etablieren und zu dokumentieren…**
- **Wenn sich für den Betroffenen aus diesem Verstoß weitere Risiken ergeben, ist er ggf. zu benachrichtigen…**

spyra@rpmed.de

Art. 34 - Meldung bei Datenschutzverletzungen

- **Bei einer „Datenpanne“ muss der Verantwortliche zwingend eine Risikoanalyse bezogen auf die Auswirkungen auf den Betroffenen durchführen.**

- **Bei dieser gilt es, insbesondere auch die Wahrscheinlichkeit zu berücksichtigen, in wie fern die Daten des Betroffenen „gegen“ ihn verwendet werden können (der Verlust wirklich verschlüsselter Daten kann die Meldepflicht entfallen lassen).**

- **Stellt der Verantwortliche jedoch fest, dass mit der Datenschutzverletzung ein hohes Risiko für den Betroffenen verbunden sein kann, muss er neben der Behörde, immer auch die Betroffenen unverzüglich informieren und „beichten“.**

- **Die Kritikalität der Datenverarbeitung lässt sich oftmals schon in einer sog. Datenschutzfolgenabschätzung ermitteln.**

spyra@rpmed.de

Art. 35 - Datenschutz-Folgenabschätzung - Vorbemerkung

- **Der risikobasierte Ansatz der VO wird auch in der sog. „Datenschutz-Folgeabschätzung" (DFA) oder „privacy impact assessment" (PIA) deutlich.**
- **Diese Pflicht kennen wir in Deutschland mehr oder weniger als „Vorabkontrolle".**
- **Eine solche ist „heute" wie „morgen" grundsätzlich durchzuführen, z. B. bei der Verwendung „neuer" Technologien, die wegen ihrer Art, des Umfangs, der Umstände und der Zwecke voraussichtlich ein hohes Risiko für die Betroffenen mit sich bringen.**
- **Und wann ist sie genau erforderlich?**

spyra@rpmed.de

Art. 35 - Datenschutz-Folgenabschätzung

- **Eine DFA ist insbesondere in folgenden Fällen erforderlich:**
  - **bei einer systematischen und umfassenden Bewertung persönlicher Aspekte (insbesondere „Profiling“)**
  - **bei der umfangreichen Verarbeitung besonderer Kategorien pbD (Artt. 9,10) oder**
  - **der systematischen, umfangreichen Überwachung öffentlich zugänglicher Bereiche (Videoüberwachung);**

- **Die Durchführung der DFA obliegt dem Verantwortlichen, der sich jedoch dem Rats des DSB (falls einer bestellt wurde) bedienen kann.**

- **Die Einbeziehung des DSB ist oftmals auch sehr hilfreich, denn bei der DFA gilt es einiges zu berücksichtigen...**

spyra@rpmed.de

Art. 35 - Datenschutz-Folgenabschätzung- Inhalt

- **In der DFA müssen zumindest folgende Bereiche behandelt werden bzw. das anzufertigende Dokument muss folgende Angaben beinhalten:**
  - **eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, ggf. berechtigte Interessen des Verantwortlichen;**
  - **Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;**
  - **eine Bewertung der Risiken für die Betroffenen und**
  - **die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und der diesbezügliche Nachweis, dass VO eingehalten wird.**
- **Und ggf. muss der Verantwortliche die Aufsichtsbehörde kontaktieren…**

spyra@rpmed.de

Art. 36 - Vorherige Konsultation

- **Ergibt die DFA, dass die Verarbeitung mit einem hohen Risiko verbunden ist und die getroffenen Maßnahmen nicht ausreichen, um das Risiko zu senken, muss er die Aufsichtsbehörde konsultieren.**

- **Falls Aufsichtsbehörde der Meinung ist, dass geplante Verarbeitung nicht im Einklang mit VO steht, insbesondere weil Risiko nicht ausreichend gewürdigt oder nicht ausreichend eingedämmt, muss sie innerhalb von fünf bis acht Wochen (Verlängerung um 6 Wochen möglich) schriftliche Empfehlungen abgeben und kann auch ihre Befugnisse (Art. 58) ausüben.**

- **Und weil Verantwortliche wie Ärzte auch verpflichtet sind, „Privacy by Design" zu gewährleisten, muss insbesondere auch die von ihnen eingesetzte Software entsprechend beschaffen / konzipiert sein...**

spyra@rpmed.de

Art. 25 – Privacy by Design / by default

- **Dem risikobasierten Ansatz folgend, gilt nunmehr, dass „Datenschutz" mit der DSGVO nun in allen Prozessen des Verantwortlichen berücksichtigt werden muss!!!**

- **Das bedeutet, dass ein MVZ in all seinen Prozessen prüfen muss, ob die „Grundprinzipien" ausreichend berücksichtigt sind.**

- **Daher gilt es insbesondere auch die eingesetzte Software hinsichtlich dieser Anforderungen zu überprüfen und ggf. mit den Herstellern der Software in Kontakt zu treten.**

- **Gerade bei Neubeschaffungen von „Software" bzw. vernetzten Produkten sollte „Privacy by Design" in den Produkten zwingend verlangt werden (wenn der Hersteller das nicht gewährleisten kann, aber trotzdem zusagt, ist sein Produkt „mangelhaft")**

- **Und weil das alles ein wenig viel war, nun eine kleine Praxishilfe!**

spyra@rpmed.de

Teil 5

Die DSGVO in einem MVZ
-
„Praxishilfe“

spyra@rpmed.de

Grundsätzliches

- **Wie aufgezeigt, kommt mit der DSGVO einiges auf uns zu.**
- **„Dreh und Angel- Punkt" von allem muss die umfassende DOKUMENTATION sein, denn es gilt:**
- **„Das, was nicht dokumentiert ist, ist auch nicht geschehen!!!"**
- **Um dem „Dschungel" an Anforderungen „Herr zu werden", sollte man sich zielführend und praxisorientiert mit den neuen Herausforderungen auseinandersetzen.**
- **Daher nun eine Reihe von Empfehlungen („Checkliste"), die Ihnen erste Empfehlungen geben soll, wie Sie „dem DSGVO-Wahnsinn" halbwegs Einhalt gebieten können..**

spyra@rpmed.de

1. Verantwortlichkeit

- **Die DSGVO legt nahe, dass Sie eine auf die Größe des MVZ zugeschnittene „Datenschutzorganisation“ aufbauen sollten.**
- **Dazu sollten insbesondere folgende Aspekte berücksichtigt werden:**
  - **Bestimmung der Verantwortlichkeiten im MVZ**
  - **Bestimmung von Prozessverantwortlichen (die Gesamtverantwortlichkeit liegt jedoch beim „Verantwortlichen)**
  - **Ggf. Bestellung eines Datenschutzbeauftragten (bei mehr als 10 Personen)**
  - **Stellen Sie sicher, dass Sie alles Relevante dokumentieren (Rechenschaftspflicht) -> Einsatz von Software sinnvoll?**
  - **Sensibilisieren Sie Ihre Mitarbeiter hinsichtlich der neuen Anforderungen und dokumentieren sie dieses!**
  - **…**
- **Und all dieses können Sie wie gesagt nur gewährleisten, bei entsprechenden „Transparenz“ über die Datenverarbeitung…**

spyra@rpmed.de

2. Transparenz (1)

- **Die Anforderungen der DSGVO wie z. B. die Pflicht zur ordnungsgemäßen Erfüllung der Betroffenenrechte, lassen sich nur abbilden, wenn man selber einen genauen Einblick in sämtliche stattfindende Datenverarbeitungen hat.**

- **Dokumentieren Sie daher insbesondere:**
  - **die eingesetzten Computer / Rechner im MVZ inkl. der darauf installierten Software,**
  - **die von Ihnen verwendeten vernetzten (Software-) Medizinprodukte,**
  - **die dienstlich genutzten Smartphones, inkl. der darauf installierten Apps**
  - **ihren Webserver,**
  - **ihren E-Mailserver,**
  - **...**

- **Und noch mehr...**

spyra@rpmed.de

2. Transparenz (2)

- **Sorgen Sie ferner dafür, dass Sie davon Kenntnis haben / bekommen,**
  - **welche Daten,**
  - **von wem,**
  - **wie,**
  - **wo bzw. auf welchen (Computer-)Systemen,**
  - **mit welcher Software,**
  - **zu welchem Zweck,**

  verarbeitet werden.

- **Erstellen Sie eine Dokumentation hinsichtlich aller (technischen und organisatorischen) Maßnahmen, die getroffen wurden, um die Computer bzw. die sonstige verwendete IT inkl. der damit verarbeiteten Daten zu schützen.**

- **Und noch mehr…**

spyra@rpmed.de

2. Transparenz (3)

- **Erstellen Sie ein (Verarbeitungs-)Verzeichnis entsprechend der gesetzlichen Anforderungen (vgl. Art. 30), in dem alle Ihre Prozesse entsprechend der gesetzlichen Vorgaben aufgelistet sind.**
- **Überprüfen sie dieses in regelmäßigen Abständen auf seine Aktualität / Vollständigkeit hin.**
- **Und dann gilt es immer zu gewährleisten, dass die Datenverarbeitung „rechtmäßig" erfolgt.**

spyra@rpmed.de

3. Rechtmäßigkeit - Gesetz

- **Prüfen Sie, ob sich alle der von Ihnen durchgeführten Verarbeitungen auf eine gesetzliche Legitimation (gesetzlich legitimierter Zweck) insbesondere**
  - **Art. 6 und**
  - **Art. 9 stützen lassen (z. B. die Datenverarbeitung zu Behandlungszwecken gem. Art. 9 Abs. 2 h)**
- **Dokumentieren sie dieses umfassend.**
- **Und besonderes Augenmerk gilt es den „Einwilligungserklärungen" zu schenken....**

spyra@rpmed.de

3. Rechtmäßigkeit - Einwilligung

- **Überprüfen Sie Ihre bisher verwendeten Patienteneinwilligungserklärungen danach, ob Sie diese überhaupt brauchen, diese konform mit dem alten Recht (z. B. BDSG) und dem neuen (DSGVO) sind (Hinweis auf Widerrufsmöglichkeit nicht vergessen).**

- **Prüfen Sie Ihre Erklärung insbesondere darauf, ob sie die Einwilligenden:**
  - **transparent**
  - **umfassend,**
  - **in einer klaren und verständlichen Form / Sprache**

  über die von Ihnen durchgeführten Datenverarbeitungen informiert.

- **Dem Patienten gilt es dabei aufzuzeigen, wer alles an der ihn betreffenden Datenverarbeitung beteiligt ist und wie, zu welchen Zwecken diese Verarbeitung erfolgt.**

spyra@rpmed.de

4. Einbindung / Beteiligung von Externen (1)

- **Verschaffen Sie sich einen Überblick, wer alles Zugriff auf die von Ihnen verarbeiteten Daten hat bzw. welchen externen Stellen Sie alles Daten übermitteln.**
- **Dabei sollten Sie insbesondere folgende Stellen berücksichtigen:**
  - **Dienstleister, die die MVZ-EDV betreuen,**
  - **zum Factoring eingesetzte Unternehmen,**
  - **etwaige Steuerberater,**
  - **DATEV,**
  - **Rechtsanwälte,**
  - **...**
- **Und noch mehr...**

spyra@rpmed.de

4. Einbindung / Beteiligung von Externen (2)

- **Prüfen Sie, ob es Geräte wie Medizinprodukte, Scanner, Faxgeräte usw. gibt, die Sie gemeinsam nutzen?**
- **Falls dieses der Fall sein sollte, gilt es zu prüfen, ob ausreichende vertragliche Regelungen (Art. 26, Art. 28) getroffen wurden, um eine mögliche Datenpreisgabe an diese Parteien zu legitimieren.**
- **Prüfen Sie, ob alle der von Ihnen mit den Externen verwendeten Verträge:**
  - **die neuen Anforderungen der DSGVO (z. B. Art. 26 oder Art. 28),**
  - **die zur ärztliche Verschwiegenheitspflicht geltenden berufsrechtlichen Landesregelungen**
  - **sowie § 203 StGB (Gesetzesänderung vom September 2017) erfüllen.**

spyra@rpmed.de

5. Sicherheit (1)

- **Bei den von Ihnen identifizierten Datenverarbeitungen Ihres MVZ, gilt es eine Risikobeurteilung vorzunehmen (aus Sicht des Betroffenen).**
- **Der besseren Übersichtlichkeit halber empfiehlt sich eine Kategorisierung der Risiken in die bekannten Ampelfarben:**
  - **grün (geringes Risiko)**
  - **gelb (mittleres Risiko)**
  - **rot (hohes / sehr hohes Risiko).**
- **Bei Datenverarbeitungen mit einem (sehr) hohen Risiko für den Betroffenen (rot), gilt es unter Umständen, eine sog. Datenschutzfolgenabschätzung entsprechend der gesetzlichen Anforderungen durchzuführen (vgl. Art. 35 und Art. 36).**

spyra@rpmed.de

5. Sicherheit (2)

- **Treffen Sie entsprechend des von Ihnen ermittelten Risikos die notwendigen Maßnahmen, um die Daten zu schützen und dokumentieren Sie dieses.**
- **Sie sollten prüfen, ob Sie bei der konkreten Datenverarbeitung z. B. in der von Ihnen verwendeten Software, Verschlüsselungs- bzw. Pseudonymisierungsverfahren einsetzen können.**
- **Ferner sollten Sie Ihren Betrieb so einrichten, dass Sie in die Lage versetzt werden, etwaige Datenschutzverstöße / Datenpannen erkennen zu können (vgl. Art. 33).**
- **Und gerade für Datenpannen gilt es einen Prozess zu etablieren…**

spyra@rpmed.de

5. Sicherheit (3)

- **Sie sollten einen Prozess definieren und dokumentieren, wie auf eine „Datenpanne" reagiert werden soll (Art. 33, 34 DSGVO). Dieser Prozess sollte insbesondere nachfolgende Fragen beantworten:**
  - **Wie lassen sich relevante Vorfälle erkennen?**
  - **Wer ist alles bei einer festgestellten „Datenpanne" zu beteiligen?**
  - **Was sind die einzuhaltenden Kommunikationswege?**
  - **Wie ist das Risiko des Vorfalls aus Sicht des Betroffenen zu ermitteln?**
  - **Wer muss alles, entsprechend der ermittelten Risikohöhe benachrichtigt werden?**
  - **...**
- **Und ganz wichtig ist die Einhaltung des „NEED TO KNOW-Prinzips...**

spyra@rpmed.de

5. Sicherheit (4)

- **Stellen Sie sicher, dass nur die Personen auf Daten zugreifen können, die sie zur Erfüllung der ihnen übertragenen Aufgaben benötigen („need to know Prinzip"). Diesbezüglich sollten Sie z.B. im Rollen- und Berechtigungssystem ihres Arztsystems festlegen:**
  - **wer,**
  - **wie,**
  - **in welchem Umfang,**
  - **zu welchen Zwecken**

  auf die entsprechenden Daten zugreifen kann.

- **Bei Fernwartungen sollten Sie darauf achten:**
  - **dass der fernwartende Mitarbeiter, immer so wenig Daten wie möglich sieht,**
  - **Sie bzw. Ihre Mitarbeiter die Fernwartungsarbeiten überwachen und**
  - **die Möglichkeit haben, bei unerwarteten Ereignissen, die Fernwartung zu beenden.**

spyra@rpmed.de

6. Patientenrechte

- **Stellen Sie sicher, dass sämtliche der in der DSGVO enthaltenen Rechte der Patienten (vgl. insbesondere Art. 12 – Art. 22) in einer angemessenen Zeit erfüllt werden können.**
- **Sie sollten diesbezüglich Prozesse etablieren, mit denen klar definiert wird, wie bspw. mit Auskunftsersuchen von Patienten verfahren werden soll.**
- **In einem solchen Prozess sollten insbesondere folgende Fragen beantwortet und dokumentiert werden:**
  - **Wer ist Prozessverantwortlicher / Wer sind die Prozessbeteiligten?**
  - **Wie ist der genaue Prozessablauf?**
  - **Wie erfolgt die Verifikation der Berechtigung des Auskunftsersuchenden?**
  - **Wie lassen sich die Daten identifizieren, für die Auskunft ersucht wird?**
  - **Wie soll die Übermittlung der Information an den Betroffenen erfolgen?**
  - **…**

spyra@rpmed.de

6. Patientenrechte

- **Stellen Sie sicher, dass besonders in Ihrem Patientenaufnahmebogen der Patient über die ihn betreffenden Datenverarbeitungen in einer klaren und verständlichen Form / Sprache unterrichtet wird (vgl. Art. 12 – Art. 14).**
- **Überprüfen Sie, ob sich Daten von Betroffenen / Patienten entsprechend der gesetzlichen Anforderungen mit der von Ihnen eingesetzten Software löschen / sperren lassen.**
- **Entwickeln Sie ein Aufbewahrungs- / Löschungskonzept.**
- **Prüfen Sie, ob unrichtige Daten von Patienten entsprechend berichtigt werden können und etablieren Sie einen Prozess entwickeln, durch den Sie auf Berichtigungsverlangen des Patienten reagieren können.**

spyra@rpmed.de

7. Mitarbeiterrechte

- **Auch Ihre Mitarbeiter sind Betroffene (wie Patienten).**
- **Zukünftig können sich Verstöße gegen den Datenschutz im Mitarbeiterverhältnis, unter Umständen noch negativer auf arbeitsgerichtliche Verfahren zwischen Ihnen und (ehemaligen) Mitarbeitern auswirken (Beweislast).**
- **Stellen Sie daher sicher, dass Sie den gestärkten Mitarbeiterbetroffenenrechten genauso wie den Patientenrechten angemessen begegnen können.**
- **Beim Einsatz von Technologien, die z. B. auch eine Mitarbeiterüberwachung ermöglichen wie etwa eine Videoüberwachung, sollten Sie vorsichtig sein und diese besonders auf ihre Datenschutzkonformität hin überprüfen (Datenschutzfolgenabschätzung?)**

spyra@rpmed.de

8. Beschaffung neuer Geräte

- **Stellen Sie sicher, dass die entsprechenden Hersteller Ihnen aussagekräftige Informationen liefern, um Sie in die Lage zu versetzen zu beurteilen, ob Sie beim Einsatz dieser Geräte weiterhin ein angemessenes Datenschutzniveau gewährleisten können.**
- **Verpflichten Sie Hersteller vertraglich, an etwaigen, von Ihnen durchzuführenden Datenschutzfolgenabschätzungen im erforderlichen Umfang mitzuwirken.**
- **Fragen Sie bei den Herstellern nach, ob und in wie weit es Ihnen möglich ist, mit den neuen Produkten „Privacy by Design und by default" zu gewährleisten (zwingende Bedingung für den Erwerb der neuen Produkte).**
- **Lassen Sie sich diesbezüglich aussagekräftige Unterlagen wie ein Datenschutzkonzept oder IT-Sicherheitskonzept von ihnen aushändigen…**

spyra@rpmed.de

FAZIT

- **Mit der DSGVO kommt einiges auf uns zu.**
- **Insbesondere ist es nun erforderlich, eine risikoorientierte Sichtweise (aus Sicht des Betroffenen) der eigenen Datenverarbeitung einzunehmen.**
- **Ferner gilt es alles Datenschutzrelevante umfassend und übersichtlich zu dokumentieren, damit man jederzeit auf diese Informationen zugreifen kann (ohne eine entsprechende Software m.A. nach „Mission impossible“).**
- **Der zu betreibende Aufwand ist jedoch das notwendige Übel, das mit der Digitalisierung einher geht.**
- **Denn es gilt, dem Betroffenen, der jeder von uns sein kann, stets den notwendigen Respekt und das zwingend erforderliche Vertrauen entgegenzubringen (Goldene Regel)!**

spyra@rpmed.de

Gibt es noch Fragen?

Gerald Spyra, LL.M.
Rechtsanwalt,
Externer Datenschutzbeauftragter

https://www.rpmed.de/

spyra@rpmed.de

Partner bei
RATAJCZAK & PARTNER mbB
Zollstockgürtel 59 / Atelier 25
50969 Köln

Vielen Dank für Ihr Interesse!

spyra@rpmed.de