Der Schutz von Daten und die EU-Datenschutzgrundverordnung

Was dieses für unser LEBEN bedeutet!

15.02.2024

Gerald Spyra, LL.M.
RP mbB
Rechtsanwälte

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:**
  Der Status Quo der „smarten", modernen Datenverarbeitung
- **Teil 2:**
  Die EU-Datenschutzgrundverordnung - Grundsätzliche Prinzipien der DSGVO
- **Teil 3:**
  Hinweise für den Umgang mit der DSGVO in der Praxis
- **Teil 4:**
  Privacy by Design
- **Fazit**

spyra@rpmed.de

Teil 1

Der Status quo der modernen, „smarten“ Datenverarbeitung…

spyra@rpmed.de

Immer mehr, vernetzte IT…

- **Immer mehr vernetzte IT bzw. „smarte Geräte“ werden in Unternehmen, Behörden, etc. 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 dem Unternehmen / uns zu tun haben, dennoch die Daten 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…**

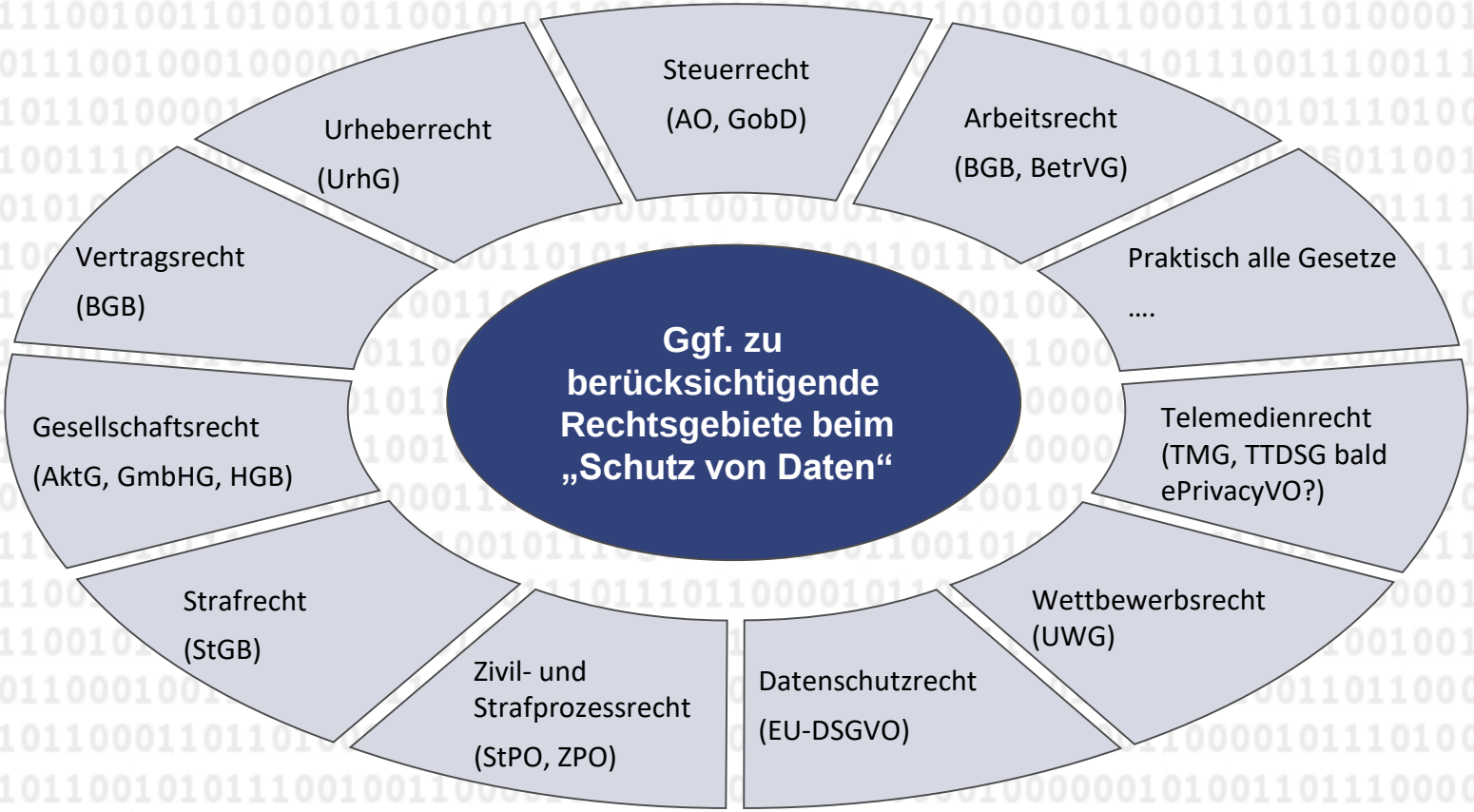
spyra@rpmed.de

Die Bedeutung der Daten und ihrer Verarbeitung

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

spyra@rpmed.de

Einblick in den “Gesetzesdschungel” im Bereich “Schutz von Daten”



- **Und gerade das Datenschutzrecht kann dazu beitragen, den Dschungel zu lichten…**

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 seiner „Ersparnisse",**
  - **zum Schutz der Gesundheit und des Lebens,**
  - **zum Schutz des „Jobs" (der Zulassung), vor dem Gefängnis,**
  - **…**
- **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.**
- **Und weil alles immer „smarter“ wird, wird bspw. die Einschätzung der Schutzbedürftigkeit von Daten immer schwieriger…**

spyra@rpmed.de

Problem Daten

- **Ein einziges Datum kann praktisch unbegrenzt viele, unterschiedliche 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, 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 die Datenschutzgrundverordnung…**

spyra@rpmed.de

Teil 2

Datenschutzgrundverordnung
–
Was ist die DSGVO
und
was hat sie für Auswirkungen?

spyra@rpmed.de

Datenschutz mit der DSGVO

- **Die DSGVO gilt in ganz Europa seit dem 25. Mai 2018 direkt (braucht grundsätzlich nicht mehr, anders als die EU-Richtlinie in nationales Recht umgesetzt werden).**

- **Sie verdrängt (in ihrem Anwendungsbereich) das bisher geltende nationale Datenschutzrecht und nur da, wo der nationale Gesetzgeber in der DSGVO ermächtigt wird, eigene Regelungen zu schaffen, finden diese zusätzlich zur DSGVO Anwendung.**

- **Die DSGVO lässt sich auf einige Grundprinzipien runterbrechen, mit denen wir uns nun beschäftigen wollen…**

spyra@rpmed.de

Grundprinzipien der Verarbeitung - Art. 5

- **In der DSGVO sind Grundprinzipien festgelegt, die für praktisch jede Verarbeitung PERSONENBEZOGENER DATEN gelten.**

- **Jede Datenverarbeitung in einem Unternehmen / Behörde / Verein usw. muss sich daher 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 rechtmäßig 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.**
- **Zur Auslegung des Gebots der „Fairness" lassen sich Analogien zu den AGB-Regelungen des BGB ziehen.**
- **Mithin darf sie für einen Betroffenen keine „Überraschungen" beinhalten (z. B. unerlaubte Datenübermittlungen usw.) und es muss ihm die Geltendmachung seiner Rechte ermöglicht werden.**
- **Eine Ausprägung des Gebot der „Fairness" sind damit die mit der DSGVO gestärkten Betroffenenrechte...**

spyra@rpmed.de

Gestärkte Betroffenenrechte

- **Den stärkeren Schutz Schutz für die Betroffenen will die DSGVO insbesondere durch die gestärkten Betroffenenrechte erreichen.**
- **Aus den gestärkten Betroffenenrechte resultieren automatisch erhöhte Pflichten des Verantwortlichen, diese umfassend zu erfüllen.**
- **Ein Verstoß gegen die Betroffenenrechte erfüllt den großen Bußgeldrahmen (bis 20 Mio. oder 4 % des Jahresumsatzes).**
- **Die Betroffenenrechte lassen sich in Kategorien einteilen…**

spyra@rpmed.de

Die unterschiedlichen Betroffenenrechte in der DSGVO

- **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 er „seine" Daten erhalten bzw. übermitteln lassen kann;**
  - **durch die er seine Daten löschen / sperren lassen kann;**
  - **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 mannigfaltigen, gestärkten Betroffenenrechte lassen sich m.A. nur mit entsprechend etablierten Prozessen, die wiederum eine umfassende Transparenz voraussetzen erfüllen...**

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 (Art. 5 Abs. 1 lit. b)

- **Schon die Erhebung von Daten, erfordert klare, eindeutig festgelegte, legitime Zwecke.**
- **Eine (Weiter-) Verarbeitung zu anderen Zwecken ist nicht gestattet, wenn kein anderer legitimer Zweck vorliegt oder 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 bei ihm und bei denjenigen, denen er die Daten übermittelt hat, 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 bitte 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 und gibt es keine weitere Legitimation zur Aufbewahrung, müssen sie folglich „gelöscht“ werden.**
- **Sie dürfen länger aufbewahrt werden zu Archivierungs-, Wissenschafts- oder Forschungs- oder statistischen Zwecken und die entsprechend erforderlichen Schutzmaßnahmen getroffen wurden.**
- **Die erforderlichen technischen und organisatorischen Maßnahmen (TOM) sind notwendig, um die Integrität und die Vertraulichkeit der Daten zu gewährleisten…**

spyra@rpmed.de

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

- **Bei der Datenverarbeitung gilt es immer, ein ausreichendes Datensicherheitsniveau zu gewährleisten (C I A).**
- **Die diesbezüglichen Schutzmaßnahmen müssen immer im angemessenen Verhältnis zum mit der Verarbeitung einhergehenden Risikos für den Betroffenen (by Design) sein.**
- **Bei Verarbeitungen mit hohen Risiken für den Betroffenen, gilt es eine spezielle Risikoanalyse vorzunehmen (Datenschutzfolgenabschätzung).**
- **Und die Erfüllung der Grundprinzipien gilt es jederzeit nachweisen zu können...**

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 und damit die Sanktionen verhindern / abmildern…**

spyra@rpmed.de

Bußgelder / Sanktionsmöglichkeiten

- **Die DSGVO hält 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 (Untersagung usw.),**
  - **Geld- bzw. Freiheitsstrafen,**
  - **Schadensersatzansprüche (materielle und immaterielle Schäden)**
  - **Abmahnungen z. B. von Verbraucherzentralen oder Mitbewerbern (Datenschutz als Marktverhaltensregel);**
  - **…**
- **Und deshalb sollte man sich überlegen, wie man als Verantwortlicher mit dieser „Evolution des Datenschutzes“ umgehen will….**

spyra@rpmed.de

Teil 3

Die DSGVO und die Pflichten von Verantwortlichen - „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"), um Ihnen erste Tips zu geben, wie Sie „dem DSGVO-Wahnsinn" halbwegs Einhalt gebieten können..**

spyra@rpmed.de

1. Verantwortlichkeit

- **Die DSGVO legt nahe, dass Sie eine auf die Größe Ihrer Organisation zugeschnittene „Datenschutzorganisation“ aufbauen sollten.**
- **Dazu sollten insbesondere folgende Aspekte berücksichtigt werden:**
  - **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 in seine Organisation stattfindenden Datenverarbeitungen hat.**

- **Dokumentieren Sie daher insbesondere:**
  - **die eingesetzte IT inkl. der darauf installierten Software,**
  - **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 Sie getroffen haben, um ihre Computer bzw. die sonstige von Ihnen verwendeten 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 (z. B. Vertragsdurchführung) und**
  - **Art. 9 stützen lassen (z. B. die Datenverarbeitung zu Behandlungszwecken)**
- **Dokumentieren sie dieses umfassend.**
- **Und besonderes Augenmerk gilt es den „Einwilligungserklärungen" zu schenken....**

spyra@rpmed.de

3. Rechtmäßigkeit - Einwilligung

- **Überprüfen Sie Ihre bisher verwendeten Einwilligungserklärungen danach, ob 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 (versetzen Sie sich in den „Einwilligenden"):**
  - **transparent**
  - **umfassend,**
  - **in einer klaren und verständlichen Form / Sprache**
  - **über die von Ihnen durchgeführten Datenverarbeitungen informiert.**
- **Dem Betroffenen gilt es dabei aufzuzeigen, wer alles (wie z. B. externe Dienstleister) 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 Ihre IT betreuen,**
  - **„outgesourcete" Dienste,**
  - **Behörden,**
  - **Versicherungen,**
  - **etwaige Steuerberater,**
  - **Rechtsanwälte,**
  - **...**
- **Und noch mehr...**

spyra@rpmed.de

4. Einbindung / Beteiligung von Externen (2)

- **Prüfen Sie, ob es IT gibt, die Sie gemeinsam mit anderen Unternehmen nutzen wie (gemeinsame Verantwortlichkeit?).**
- **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),**
  - **Etwaige geltende berufsrechtliche Regelungen,**
  - **...**

  erfüllen.

spyra@rpmed.de

5. Sicherheit (1)

- **Bei den von Ihnen identifizierten Datenverarbeitungen Ihres Unternehmens, 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 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. Betroffenenrechte (1)

- **Stellen Sie sicher, dass sämtliche der in der DSGVO enthaltenen Rechte der Betroffenen (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 Betroffenen 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. Betroffenenrechte (2)

- **Stellen Sie sicher, dass besonders in Ihrem Informationsbögen der Betroffene 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 entsprechend der gesetzlichen Anforderungen mit der von Ihnen eingesetzten Software löschen / sperren lassen.**
- **Entwickeln Sie ein Aufbewahrungs- / Löschungskonzept.**
- **Prüfen Sie, ob unrichtige Daten 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 Mitarbeiter sind Betroffene!**
- **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 und entwickeln Sie diese Produkte dementsprechend…**

spyra@rpmed.de

Teil 4

Privacy by Design

„Ein Buch mit sieben Siegeln“?

spyra@rpmed.de

Art. 25 – Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

- **Privacy by Design oder Data protection by Design hat sich zu einem regelrechten Hype in den Medien entwickelt.**
- **Man liest und hört immer häufiger, wie wichtig es ist, dass die Hersteller von Hard- und Software endlich Datenschutz und Datensicherheit in ihre Geräte einbauen.**
- **Vielfach wird ihnen auch eine entsprechende Verpflichtung zugeschrieben…**
- **Und auch die Aufsichtsbehörden äußern sich immer häufiger zu diesem Thema…**

spyra@rpmed.de

„Privacy by Design“ – Aus der Praxis…

- **Aus einem Tätigkeitsbericht einer Datenschutzaufsichtsbehörde, der sich mit der VO auseinandersetzte:**
- **„[…] *Wenn Hersteller* (durch die VO) *zu datenschutzfreundlichen Produkten und Voreinstellungen gesetzlich verpflichtet werden, stärkt dies die Datenschutzrechte der Betroffenen.*“**
- **Stimmt das wirklich?**
- **Schauen wir uns das mal an…**

spyra@rpmed.de

„Privacy by Design“- Das, wonach es aussieht?

- **Um das Prinzip von „Privacy by Design“ bzw. „data protection by design“ nachvollziehen zu können, ist es zunächst essenziell zu klären, wer eigentlich in der VO zu „data protection by design“ verpflichtet wird.**
- **Ginge man zunächst nur von dem Begriff aus, würde man schnell den Herstellern die Verantwortung für „data protection by design“ in ihren Produkten zuweisen…**
- **Doch das würde der Systematik des Datenschutzrechts zuwider laufen, wonach primär der Verantwortliche und sekundär der Auftragsverarbeiter Verpflichteter ist…**
- **Und so sieht das auch die VO…**

spyra@rpmed.de

Das sagt die Verordnung in Art. 25 Abs. 1

- **So heißt es in Art. 25 Abs. 1:**
- ***„Unter Berücksichtigung des Stands der Technik und der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die persönlichen Rechte und Freiheiten trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung angemessene technische und organisatorische Maßnahmen – wie z. B. Pseudonymisierung –, mit denen die wirksame Umsetzung der Datenschutzgrundsätze wie etwa Datenminimierung und die Aufnahme der notwendigen Garantien in die Verarbeitung erreicht werden sollen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.“***

spyra@rpmed.de

Art. 25 Abs. 1 zusammengefasst…

- **Letztendlich sagt Art. 25 Abs. 1 ganz klar, dass der Verantwortliche derjenige ist, der „data protection by design" in seiner Organisation implementieren muss.**
- **Er ist derjenige, der für die Ordnungsgemäßheit der Datenverarbeitung verantwortlich ist.**
- **Daher muss er konsequentermaßen seine Unternehmensprozesse analysieren und die entsprechenden erforderlichen technischen und organisatorischen Maßnahmen (by Design) in seine Prozesse implementieren (Risikomanagement).**
- **Und dabei gilt es immer auch die Kosten und den Nutzen zu beachten (Wirtschaftlichkeit)…**

spyra@rpmed.de

Und der Hersteller???

- **Das sagt uns EG 78:**

- ***„In Bezug auf Entwicklung, Auslegung, Auswahl und Nutzung von Anwendungen, Diensten und Produkten, die entweder auf der Verarbeitung von personenbezogenen Daten beruhen oder zur Erfüllung ihrer Aufgaben personenbezogene Daten verarbeiten, sollten die Hersteller der Produkte, Dienste und Anwendungen ermutigt werden,***

das Recht auf Datenschutz bei der Entwicklung und Auslegung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen,
dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen.“

spyra@rpmed.de

Und was sagt uns das? (1)

- **Hersteller sind (wenn sie nicht selber Verantwortliche sind) grundsätzlich nicht gesetzlich verpflichtet, datenschutzfreundliche Technik zu entwickeln.**
- **Verpflichteter by „data protection by design" ist und bleibt in erster Linie der Verantwortliche.**
- **Aus diesem Grund ist er verpflichtet sicherzustellen, dass seine Verfahren „data protection by design" ausreichend berücksichtigen und muss dieses gerade auch bei Neusystemen bspw. im Rahmen einer Datenschutzfolgeabschätzung gem. Art. 35 (Vorabkontrolle) überprüfen..**
- **Bei Neuanschaffungen sollte deshalb „data protection by design" in (öffentlichen) Ausschreibungen / Anforderungsprofilen unbedingt immer berücksichtigt werden (EG 78).**

spyra@rpmed.de

Und was sagt uns das? (2)

- **Durch die gesetzliche Pflicht des Verantwortlichen zum Einsatz „datenfreundlicher Technik" soll m.A. nach ein mittelbarer Druck auf die Hersteller entstehen.**
- **Dieses insbesondere deshalb, weil durch die Regelungen der VO, der Verantwortliche theoretisch keine (Neu-) Produkte ohne bzw. mit unzureichender „data protection by design" kaufen bzw. einsetzen darf…**
- **Neusysteme, die kein „data protection by design" implementiert haben, dürften deshalb (nach Intention des Gesetzgebers) nicht mehr nachgefragt werden, so dass sich das alles optimaler Weise durch die „Macht des Marktes" von alleine regeln wird (ob das auch so funktioniert bleibt abzuwarten)…**
- **Und was gilt für „Altsysteme"…?**

spyra@rpmed.de

Und was machen wir mit den Altsystemen?

- **Legt man die Regelungen der VO eng aus, lässt sich daraus ableiten, dass man als Verantwortlicher seine Alt-Systeme danach überprüfen muss, ob mit diesen die Anforderungen nach „data protection by design" erfüllt werden können…**
- **Daher sollte man gerade für „kritische" Alt-Produkte, mit denen bspw. Gesundheitsdaten verarbeitet werden eine gründliche Prüfung vornehmen (heute im Rahmen einer verstärkten „Vorabkontrolle").**
- **Die „Wirtschaftlichkeit" sollte jedoch immer gewahrt bleiben.**
- **Bei „Mängeln" sollte man diese offen mit den Herstellern diskutieren und gemeinsam Lösungen entwickeln…**
- **Nach der VO sollte ferner in allen Geräten „data protection by default" enthalten bzw. umsetzbar sein.**

spyra@rpmed.de

„Data protection by Default“

- **So heißt es in Art. 25 Abs. 2:**
- ***„Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden;***
  dies gilt für den Umfang der erhobenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit.

- ***Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten grundsätzlich nicht ohne Eingreifen einer natürlichen Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.“***

spyra@rpmed.de

Und was bedeutet diese Regelung?

- **Ein Verantwortlicher sollte seine Soft- und Hardware deshalb danach überprüfen, ob man damit „datenschutzfreundliche Voreinstellungen“ vornehmen bzw. entsprechend erforderliche Maßnahmen umsetzen kann.**
- **Anwender sollten sich durch diese Voreinstellungen weniger Gedanken um die Einhaltung des Datenschutzes bei der Anwendung machen müssen.**
- **Und all das gilt es im Ernstfall nachweisen zu können…**

spyra@rpmed.de

Und wie kann man „data protection by design / by default“ nachweisen…?

- **Art. 25 Abs. 3:**

„Ein genehmigtes Zertifizierungsverfahren gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in den Absätzen 1 und 2 genannten Anforderungen nachzuweisen.“

- **Bezieht sich jedoch auch wiederum auf die entsprechenden Verfahren bei dem Verantwortlichen.**

- **Und was bedeutet das nun für die Hersteller von Software?**

spyra@rpmed.de

(Neue) Rechtliche Implikationen aus „privacy by design“

- **Durch die Neuerungen der DSGVO weiß man, was notwendig ist, um „compliant“ zu sein.**
- **Mithin gilt es zu evaluieren, was die zwingenden Anforderungen an die SW sind und dieses im Design umzusetzen.**
- **Daher sollte man die 8 Designstrategien ernstnehmen…**

spyra@rpmed.de

Acht Strategien beim Design (1)

- **„(Daten-) Minimierung" z. B. Bevor man verarbeitet, genau überlegen; „Anonymisierung und Pseudonymisierung,...**
- **„Verstecken" – z. B. Verschlüsseln, Verstecken von Datenflüssen, Nichtanzeigen von Daten, Anomymisieren und Pseudonymisieren,...**
- **„Separieren / Trennen" z. B. Umsetzung des „Need to know-Prinzip", Speicherung in unterschiedlichen Tabellen, Rollen und Berechtigungskonzept,...**
- **„Sammeln" – z. B. nur immer soviel sammeln, wie zur Zweckerfüllung nötig, „anonymisieren", „pseudonymisieren" usw.**

spyra@rpmed.de

Acht Strategien beim Design (2)

- **„Informieren“ – z. B. durch Erklärungen / Dokumentationen Transparenz über Datenverarbeitung und die „Betroffenenrechte“ schaffen,…**
- **„Kontrollieren“, z. B. Nutzern / Betroffenen weitestgehend die Kontrolle über die Datenverarbeitung geben, z. B. P3P-Framework,…**
- **„Durchsetzen“, z. B. Das Design anhand einer Datenschutzpolicy ausrichten, Zugangskontrollen, Rollen und Berechtigungskonzepte, usw.**
- **„Demonstrieren“, z. B. Zeigen, dass man datenschutzkonform verarbeitet (Whitepaper usw.) – Prüfen, dass man Kontrolle hat, Logging, Audits…**

spyra@rpmed.de

FAZIT

- **Mit der DSGVO ist einiges auf uns zugekommen.**
- **Es gilt, eine risikoorientierte Sichtweise (aus Sicht des Betroffenen) einzunehmen.**
- **Ferner gilt es, alles Datenschutzrelevante umfassend und übersichtlich zu dokumentieren, damit man jederzeit auf diese Informationen zugreifen kann.**
- **Der mit der DSGVO zu betreibende Aufwand ist das notwendige „ÜBEL", das mit der Digitalisierung einher geht („die bittere Pille, die es zu schlucken gilt").**
- **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