RATAJCZAK & PARTNER mbB

Die „Sicherheit“ im rechtlichen Kontext

ITSA 2019 – 09.10.2019

Ihr Referent

Gerald Spyra, LL.M.

- Partner / Rechtsanwalt
- Hohe Affinität für die Informationssicherheit

Spezialisiert auf

- das Informations- / Datenschutzrecht,
- das „Software-Medizinprodukterecht“ und
- die „IT-Forensik“

- Externer betrieblicher Datenschutzbeauftragter

RP RECHTSANWÄLTE

RATAJCZAK & PARTNER mbB

Berlin · Essen · Freiburg i.Br. · Köln · Meißen · München · Sindelfingen

www.rpmed.de

KRITIS – Das IT-SiG und das Drumherum – Ein paar einführende Worte

- Bevor man sich mit **KRITIS**, dem IT-SiG, etc. auseinandersetzt, sollte man sich zunächst einige **Fragen** stellen.
- So gilt es sich bspw. zu **fragen**:
  - **Wieso** haben wir eigentlich die **Kategorisierung** in KRITIS? Macht diese **Sinn**?
  - Was ist mit den anderen **Unternehmen**, die zwar **nicht KRITIS** sind, die aber **eng** mit **KRITIS-Unternehmen zusammenarbeiten** und munter **Daten austauschen**?
  - **Brauchen** wir diese ganzen (neuen) **Gesetze** / **Regelungen** eigentlich?
  - **Kann** es durch diese neuen **Gesetzen** (alleine) wirklich **besser werden**?
  - Müssten wir nicht **insgesamt umdenken**, um wirklich die **Sicherheit** zu **verbessern**?
  - **Adressieren** wir mit **KRITIS** die **Richtigen**?
- Bei der **Beantwortung** der Fragen ist es **zwingend erforderlich**, **offen** und **ehrlich** zu sein.
- Ein **Verschließen** vor der **Realität** ist **kontraproduktiv** und **adressiert** nur **Symptome** aber **nicht** die **Ursache**!
- Zur **Beantwortung** dieser **Fragen**, sollte man sich zunächst kurz mit dem „**status quo**“ der **Datenverarbeitung** **auseinandersetzen**….

IMMER MEHR IT…

- Wir **verlassen** uns sowohl im **Privaten** aber besonders auch im **Dienstlichen** immer mehr auf die **Datenverarbeitung von** und **mit IT** (Soft- und Hardware).
- **Alles** soll miteinander **vernetzt** werden, wodurch die **Datenverarbeitung** immer **komplexer** und **intransparenter** wird (**IoT** bzw. **IoT / IoS**).
- Wir **verlassen** uns für die **Abbildung** unserer **Geschäftsprozesse** der **realen Welt** immer mehr auf die für uns **fremde**, **digitale Datenverarbeitung** in der **virtuellen Welt**.
- **Zwangsläufig** wird damit diese **Datenverarbeitung** immer **geschäftskritischer**.
- Ein Ausfall der **Verarbeitungsmöglichkeit** oder das **Abhandenkommen** von **wichtigen Daten** kann deshalb gerade bei **KRITIS** ziemlich **„kritisch“ werden**…

KRITIS – Besonders „kritisch“

- **KRITIS-Organisationen charakterisiert**, dass der **Ausfall** ihrer **IT-Infrastruktur** und damit auch ihrer **Datenverarbeitung**, **kritisch** für die **Gesellschaft** sein können.
- Gerade weil ihre **Leistungen** so **„kritisch“** sind, ist die **Erwartungshaltung** an die **Verfügbarkeit** der **IT** und die **Gewährleistung** der **korrekten Datenverarbeitung** von **Gesetzes** wegen **hoch**.
- Daher müssen bspw. **KRITIS-Unternehmen** auch (vermeintlich) **mehr** und **höhere Anforderungen** erfüllen, als **Nicht-KRITIS-Unternehmen** (daher wird auch immer gerne **„wild“ runtergerechnet** ;).
- Es wird jedenfalls immer **deutlicher**, dass die **Bedeutung** von **Daten** bzw. der **ordnungsgemäßen Datenverarbeitung** immer **relevanter** wird…

Die Bedeutung von Daten bzw. ihrer Verarbeitung

- Auch wenn wir **unterschiedliche Begrifflichkeiten** verwenden (dazu gleich mehr), dürfte klar sein, dass **IT / Digitalisierung** bedeutet, dass **DATEN verarbeitet** werden **müssen**.
- Das wiederum bedeutet, dass je **mehr** wir uns auf **Datenverarbeitung verlassen**, umso **größer** ist das **Risiko verlassen** zu **sein** , wenn die **Datenverarbeitung nicht möglich** ist.
- **Fehlen Daten**, kann auf **Daten** nicht mehr **zugegriffen werden**, oder wurden **Daten verändert**, kann dieses **massive Auswirkungen** auf die **Datenverarbeitung** und damit die **„Sicherheit“** haben.
- Daher ist es ja **nur denklogisch konsequent**, dass je mehr wir uns auf die digitale **Datenverarbeitung verlassen**, es umso **wichtiger** wird, dass diese **„sicher“ abläuft**…

Die erhöhten Anforderungen an die „Sicherheit“

- Je **kritischer** die **Datenverarbeitung** für den **Einzelnen** und ganz besonders für die **Bevölkerung** ist, umso **wichtiger** ist die **Gewährleistung** einer ausreichenden **„Sicherheit“**.
- Dabei ist es essenziell, sich besonders mit den **Bereichen „C I A“ offen** und **ehrlich auseinanderzusetzen**.
- Dabei gilt es sich zu **vergegenwärtigen**, dass es einen **„one size fit all Ansatz“ nicht geben** kann.
- Vielmehr ist eine **risikoorientierte Herangehensweise**, die jedoch erst bei einer **entsprechenden Transparenz** über die **Datenverarbeitungen** und ihre **Umstände möglich** ist (bei **hochkomplexen Datenverarbeitungen „mission impossible“**), absolut essenziell.
- Und dann sollte man sich auch vor den **unterschiedlichsten Begrifflichkeiten der „Sicherheit“** hüten….

Die verwirrenden Begrifflichkeiten im Bereich „Sicherheit“

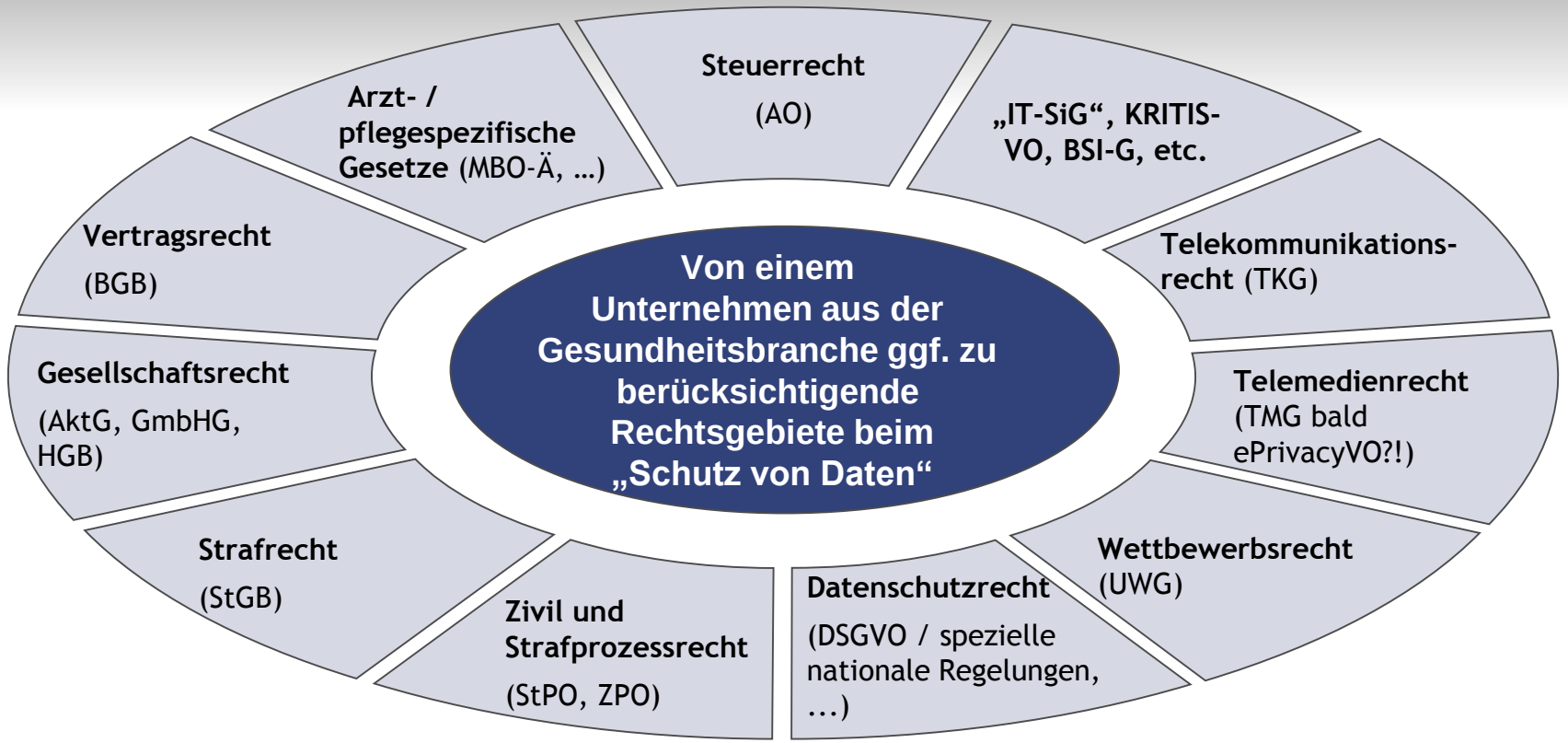
- Das Thema **„Schutz von Daten“** ist **sehr komplex**. Es werden gerade in diesem **Bereich** viele **unterschiedliche Begrifflichkeiten inflationär** und oftmals sogar **synonym** verwendet wie:
  - **Informationssicherheit**;
  - **IT-Sicherheit**;
  - **Internetsicherheit**;
  - **„Sicherheit“** (z. B. bei **Medizinprodukten**)
  - **Datenschutz / Datensicherheit**
  - **…**
- Es werden gerade im Bereich „Schutz von Daten“ immer **neue Begrifflichkeiten erfunden**, **ohne** sie jedoch jemals klar bzw. **nachvollziehbar definiert** zu **haben**.
- Und das **Schlimmste** bei all dem ist, dass immer mehr **ge „CYBER(T)“** wird.
- Die bestehenden **unklaren** sowie die immer neu **hinzukommenden**, nicht klar definierten **Begrifflichkeiten** haben zunehmend **sichtbare Auswirkungen**…

Die verwirrenden Begrifflichkeiten und ihre Konsequenzen

- Durch die vielen **Begrifflichkeiten** und ihre **synonyme Verwendung** wissen wir oftmals z.B. **nicht**:
  - **Was** diese **Begriffe** überhaupt **bedeuten** (sollen),
  - **welchen** (**Schutz-**) **Bereich** sie **betreffen**,
  - **wie** die **Hierarchie** der **Begrifflichkeiten** ist,
  - wer, **wofür** eigentlich **verantwortlich** ist,
  - **wer**, wofür im **Schadensfall haftet**,
  - wer für die **Aufsicht zuständig** ist (bspw. für die Sicherheit in Software-Medizinprodukten),
  - …
  - ???

- Gerade weil der **Schutz** von **Daten** immer **wichtiger** wird, sollte man ihn **ganzheitlich** sehen.
- Man sollte sich ferner auch darüber im Klaren sein, dass es aufgrund der **Relevanz** der **Datenverarbeitung** in der **heutigen Welt**, weitaus mehr **Gesetze** / **gesetzliche Bereiche** gibt, in denen der „**Schutz von Daten**“ eine **Rolle** spielt.

Ein Blick in den „Gesetzesdschungel“



Und besonders der „Datenschutz" erlangt durch die DSGVO eine ganz neue Qualität…

Lösung für den „Gesetzeswirrwarr“

- Bei dem ganzen **Begriff-** und **Gesetzeswirrwarr** gilt es mehr denn je, die **Sache ganzheitlich** zu betrachten.
- Daher ist es **dringend angezeigt**, ein ganzheitliches **„Schutz von Daten“ Managementsystem** aufzubauen, mit dem all die **einschlägigen gesetzlichen Regelungen** adressiert werden.
- Die **DSGVO** kann **diesbezüglich** eine **gute Basis** bieten.
- Es ist **notwendiger** denn je, **risikoorientiert** die Sache zu **betrachten**.
- Daher nun noch ein kleines **Fazit**…

Fazit

- **KRITIS** macht aus, dass die **Datenverarbeitung „systemkritisch“** ist.
- Mithin kann die **fehlende Möglichkeit** der **Datenverarbeitung** bzw. eine **fehlerhafte Datenverarbeitung** extreme **Auswirkungen** für **Betroffene** und sogar die **Bevölkerung** haben.
- Gerade weil diese **Datenverarbeitung** immer **systemkritischer** wird, **wachsen automatisch** die **rechtlichen Anforderungen** und es entsteht ein **kaum überschaubarer Gesetzesdschungel**.
- Es gilt einen **ganzheitlichen Ansatz** zu verfolgen, bei dem die **rechtlichen**, **technischen** und **organisatorischen Implikationen gleichermaßen** berücksichtigt werden.
- Die **DSGVO** bietet eine **große Chance**, **Transparenz** in seine **Unternehmensprozesse** zu **bringen** und sie zu **optimieren**.
- Gerade weil von **KRITIS-Unternehmen systembedingt** als **risikobehafteter** angesehen werden, gilt es hier **noch genauer vorzugehen**.
- Die **ganzheitliche Beachtung** des **„Schutzes von Daten“** ist **notwendig**, um letzten Endes dem **Betroffenen** / der **Bevölkerung**, den **notwendigen Schutz** zu **geben** und **Respekt** zu **erweisen** (**„Goldene Regel“**).

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!