Rödl & Partner

PRAXISPROBLEME und PRAXISLÖSUNGEN im DATENSCHUTZ

–

Eine Zwischenbilanz nach fünf Monaten DSGVO

Christoph Naucke

Nürnberg, 8.11.2018

AGENDA

01 **Rödl & Partner**

02 **DS-GVO: Wie heiß wird die Suppe gegessen, die da gekocht wurde?**

03 **Klassische Praxisprobleme für Krankenhäuser und Pflegeeinrichtungen**

04 **Herausforderung Datenschutzfolgenabschätzung**

05 **Stolperfallen**

ÜBER UNS

ÜBER UNS

ERFOLGSGESCHICHTE AUS DEUTSCHLAND

- 1977 Gründung als Ein-Mann-Kanzlei in Nürnberg
- 2018 weltweit 4.700 Mitarbeiterinnen und Mitarbeiter in 51 Ländern mit 111 eigenen Niederlassungen
- EIN Unternehmen, kein Netzwerk oder Franchise-System
- Alles aus einer Hand: Rechtsberatung, Steuerberatung, Steuerdeklaration und BPO, Unternehmens- und IT-Beratung, Wirtschaftsprüfung
- Spezialisiert auf deutsche international tätige Unternehmen
- Eigene Unit mit Spezialisierung auf die Gesundheits- und Sozialwirtschaft, Standorte Nürnberg & Köln

DS-GVO: WIE HEIß WIRD DIE SUPPE GEGESSEN, DIE GEKOCHT WURDE?

a) Was ist eigentlich am Ende neu – und was nicht?
b) Bußgelder – im Allgemeinen und im Gesundheitswesen speziell.
c) Abmahnungen sind überwiegend Panikmache

DATENSCHUTZ 2018: WAS HAT SICH NICHT GEÄNDERT?

Seit dem 25.05.2018 ist die DSGVO rechtswirksam

Wichtige Regelungen, die in vergleichbarer Form bereits vorher bestanden:

- Prinzip der Datensparsamkeit
- Prinzip der Zweckbindung
- Prinzip der Richtigkeit, der Integrität und der Datensicherheit
- Pflicht zur Bestellung eines (betrieblichen) Datenschutzbeauftragten
- Führen eines internen Verfahrensverzeichnisses
- Einrichtung technischer und organisatorischer Maßnahmen zur Gewährleistung des Datenschutzes („TOM‘s“)
- uvm.

DATENSCHUTZ 2018: WAS TATSÄCHLICH NEU IST

Folgende Änderungen sind besonders wichtig:

- Rechenschaftspflicht und Art. 5 Abs. 2 Beweislastumkehr
- Erheblich verschärfte Bußgeldvorschriften (bis zu EUR **20 Mio.** bzw. **4 % des Umsatzes**)
- Umfangreichere **Informationspflichten**, insbesondere auch, wenn Erhebung nicht direkt beim Betroffenen erfolgt, sowie anspruchsvolle Anforderungen an Verständlichkeit und Zugänglichkeit
- Führen eines (detaillierten) **Verarbeitungsverzeichnisses**. Pflicht zur Führung des Verzeichnisses geht über vom betrieblichen Datenschutzbeauftragter auf den Verantwortlichen, faktisch also auf den gesetzlichen Vertreter
- **Betrieblicher Datenschutzbeauftragter** erhält dafür umfassendere Überwachungspflichten. Daraus leitet sich wohl auch eine Garantenstellung des DSB im Umfang seiner Aufgaben ab. Er wird faktisch dazu gezwungen, bei Verstößen nachdrücklicher zu sein
- Pflicht zur ausführlichen **Datenschutz-Folgenabschätzung** bei Verarbeitungstätigkeiten, die besondere Risiken für die Betroffenen bedeuten
- **Meldepflicht** für Datenpannen innerhalb **von 72 Stunden**
- Wesentlich konkreter formulierte **Betroffenenrechte** (Berichtigung, Löschung, Auskunft, Widerspruch, Übertragbarkeit)
- **Löschkonzept** muss **dokumentiert** und **umgesetzt** sein
- Neu eingeführter Rechtsgrund „**berechtigte Interessen**“ weicht die restriktiven Regelungen in Bezug auf Werbung auf. Allerdings umfassende Dokumentationspflichten des Verantwortlichen und „Opt-Out“ Erfordernis in jedem Fall.

BUßGELDER – IM ALLGEMEINEN

Bußgelder nach Art. 83 Abs. 4:

Geldbußen von bis zu **10 Mio. EUR** oder von bis zu **2 %** des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs u.a. bei…

- Verletzung der besonderen Schutzrechte von Kindern
- Fehlen datenschutzfreundlicher Voreinstellungen
- Fehlen des Verarbeitungsverzeichnisses
- Fehlen notwendiger Vereinbarungen zur Auftragsverarbeitung
- Fehlende Datenschutzfolgenabschätzung
- Nicht erfolgte Meldung eines Datenschutzverstoßes

Bußgelder nach Art. 83 Abs. 5 und 6:

Geldbußen von bis zu **20 Mio. EUR** oder im Fall von bis zu **4 %** des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs u.a. bei…

- Verstößen gegen Grundsätze der Verarbeitung
- Nichteinhaltung der Betroffenenrechte
- Unzulässige Datenübermittlung in ein Drittland
- Nichtbefolgen von Anweisungen der Datenschutzbehörden

BUßGELDER IM GESUNDHEITSWESEN

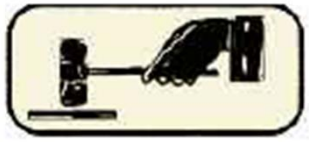
Frankfurter Allgemeine

400.000 Euro Strafe für DSGVO-Verstoß

In Portugal droht einem Krankenhaus das erste beträchtliche Bußgeld wegen eines Verstoßes gegen die Datenschutzgrundverordnung.

Laut dem Zeitungsbericht hat der Krankenhausbetreiber Untersuchungen der Datenschützer zufolge „bewusst“ IT-Technikern Zugang zu Daten verschafft, die eigentlich nur von Ärzten hätten eingesehen werden dürfen. Durch einen Test sei festgestellt worden, dass solch ein Profil mit unbegrenztem Zugang problemlos erstellt werden konnte.

ABMAHNUNGEN SIND ÜBERWIEGEND PANIKMACHE



Gerichte uneins über DSGVO

Können Verstöße gegen die Datenschutz-Grundverordnung (DSGVO) nun abgemahnt werden oder nicht? Diese auch politisch sehr umstrittene Frage wird von Gerichten bislang uneinheitlich beantwortet. Das Landgericht (LG) Würzburg hatte einen Unterlassungsanspruch kürzlich zugelassen (Az.: 11 O 1741/18, F.A.Z. vom 26. September). Das LG Bochum entschied dagegen, dass solche Verstöße nur durch die Verordnung selbst bestraft werden könnten und diese insofern abschließend sei (Az.: I-12 O 85/18). Die Richter schlossen sich damit einem Standardkommentar zum Gesetz gegen unlauteren Wettbewerb (UWG) an. Am Freitag hatte der Bundesrat eine Initiative abgelehnt: Bayern wollte wettbewerbsrechtliche Ansprüche gesetzlich ausschließen, was allerdings auch den Verbraucherschutzverbänden Klagemöglichkeiten genommen hätte. hw.

Die Grundlage für die Abmahnung muss i.d.R. aus dem Wettbewerbsrecht (UWG) hergeleitet werden.

STANDARD-DOKUMENTE UND DEREN UMSETZUNG IN KRANKENHAUS UND PFLEGEEINRICHTUNG

a) Verarbeitungsverzeichnis
b) TOM’s

BEISPIEL FÜR DEN AUFBAU EINES VERARBEITUNGSVERZEICHNISSES

1. **HAUPTBLATT**
2. **GRUNDSTRUKTUR**
3. **VERARBEITUNGSTÄTIGKEITEN (Bsp. Krankenhaus)**
   - 3.1 Patientenaufnahme
   - 3.2 Stationäre Behandlung
   - 3.3 Kliniken
   - 3.4 Unterstützungsfunktionen
   - 3.5 Administrative Funktionen
4. **ALLGEMEINE TOM'S**
5. **IT-SYSTEME UND SYSTEMBEZOGENE TOM'S**
   - 5.1 Übersicht der Systeme
   - 5.2 Details zu den Anwendungen
6. **DATENSCHUTZ-PROZESSE**
   - 6.1 Datenschutzverletzungen
   - 6.2 Konzept zur Datenschutzfolgenabschätzung
   - 6.3 Dokumentation der Sensibilisierungsmaßnahmen

BEISPIELHAFTER KAPITELAUFBAU ZU EINER VERARBEITUNGSTÄTIGKEIT

- Datum, ausfüllende Person
- Bezeichnung der Verarbeitung
- Beginn der Verarbeitung, Historie
- Grundsätzliche Angaben zur Verarbeitung und zur Verantwortlichkeit
- Interne Ansprechpartner und Organisationseinheit
- Ggf. Name u. Anschrift des Auftragnehmers, wenn Auftragsverarbeitung
- Zweck der Verarbeitungstätigkeit
- Rechtsgrundlage der Verarbeitungstätigkeit (z.B. mit Checkboxen)
- Kreis der betroffenen Personen (z.B. mit Checkboxen)
- Art der Daten / Datenkategorien (z.B. mit Checkboxen)
- Datenweitergabe und deren Empfänger: Interne und externe Empfänger und Dritte
- Geplante Datenübermittlung in Drittstaaten (außerhalb der EU)
- Regelfristen für die Löschung der Daten, gesetzliche Aufbewahrungsvorschriften, ggf. vorhandene Löschkonzepte
- Mittel der Verarbeitung: eingesetzte Software bzw. Systeme (Ziel: systembezogene TOMs dort abbilden)
- Technische und organisatorische Maßnahmen (Art. 32 DSGVO): Dreigliedriger Aufbau (vgl. weiter unten)
- Datenschutz-Folgenabschätzung ja/nein

NIVEAU DER TOM‘S: WUNSCH UND WIRKLICHKEIT

Thema	Typischer Praxiszustand, jedoch nicht ausreichend	Erforderliche Verbesserung, um ein gemeinhin akzeptiertes Mindestmaß an TOM’s zu erreichen
Gruppenpasswörter	Es werden Gruppenpasswörter (z.B. eines für die ganze Station) eingesetzt	Ausschließlich persönliche LogIns, Verbot der Passwort-Weitergabe.
Bildschirmsperre	Keine automatisierte Bildschirmsperre	Einstellung automatischer Bildschirmsperre
Forschung	Patientendaten werden auf Anforderung uneingeschränkt zu Forschungszwecken zur Verfügung gestellt	Prüfung inwiefern tatsächlich der gesamte Datensatz erforderlich ist. Möglichst pseudonymisieren. Landesrecht beachten!
Versand von Patientenunterlagen	Zum Teil per Fax ohne Sicherstellung der korrekten Zieleingabe sowie fehlende Nachkontrolle	Persönliche Übergabe an Patienten, Postweg (Vermerk „Vertraulich“), per Email als verschlüsselter Anhang ohne personenbezogene Daten im Betreff oder Email-Text. Per Fax nur in Ausnahmefällen (Abstimmung Sendezeitpunkt, direkte Entgegennahme, …)
Pfortenauskunft	Keine Prüfung der Einwilligung des Patienten, keine Identifikation der Besucher	Einführung eines Prozesses zur Sicherstellung der Berechtigung (Passwortvereinbarung mit Patient, Authentifizierungsverfahren oder keine Auskunft …)
Kontrolle der Fernwartung von Anwendungen	Offene Kommunikationskanäle für den Dienstleister, uneingeschränkter Zugriff	Bedarfsgerechte Freischaltung sowie Kontrolle (Überwachung durch Mitarbeiter)

PRAGMATISCHE MÖGLICHKEITEN ZUR DOKUMENTATION DER TOM‘S

Modell einer dreigliedrigen Abbildung

Unternehmensbezogene TOMs	Verarbeitungsbezogene TOM‘s	Systembezogene TOM‘s
Beispiele: - Zutrittsregelung und Zutrittsbeschränkung - Datenschutzrichtlinie - Rechenzentrum und dessen Sicherung - Usw. … - Dokumentation solcher TOM‘s erfolgt übergreifend	- Beispiel: Prozessbezogene Dienstanweisungen, abteilungsspezifische Zutrittsregelungen - Erfassung erfolgt im Kontext der Prozessaufnahme / der einzelnen Verarbeitungstätigkeit	- Beispiel: Rechte- und Rollenkonzepte der verwendeten Anwendungen, Passwortrichtlinien - Erfassung im Rahmen der Erfassung der Systemlandschaft - Dokumentation im Rahmen der Softwareaufstellung

KLASSISCHE PROBLEME AUS DER PRAXIS BEI KRANKENHÄUSERN UND PFLEGEEINRICHTUNGEN

a) Krankenhaus: Gemeinsame KIS-Nutzung mehrerer Rechtsträger
b) Wo braucht es eine Vereinbarung zur Auftragsverarbeitung – und wo *nicht*?
c) Wo braucht es eine Einwilligungserklärung – und wo *nicht?*
d) Patientenakten: Umgang mit der „Gewahrsams“-Anforderung des BayKrG

GEMEINSAME KIS-NUTZUNG MEHRERER RECHTSTRÄGER

Speziell für den Bereich der **Krankenhausinformationssysteme** haben die Datenschutzbeauftragten des Bundes und der Länder sowie kirchliche Datenschutzbeauftragte die „Orientierungshilfe Krankenhausinformationssysteme“ herausgegeben. Die aktuelle Version stammt aus dem Jahr 2014 und stellt insofern einen generellen Erwartungshorizont der Aufsichtsbehörden bzgl. KIS-Systemen dar.

Häufig nutzen mehrere Rechtsträger gemeinsam ein Patienteninformationssystem (Klinikum & MVZ, Pflegekonzerne, usw.)

Anspruchsvolle Anforderungen	OH-KIS Textziffer (Technische Anforderungen)
- Umsetzungsdokumentation des Berechtigungskonzeptes	4.4
- Mandantenfähigkeit des KIS	1.2
- Berechtigungsvergabe im Verarbeitungskontext	3.2
- Fernwartungen müssen kontrollierbar sein	8.2

ROLLENKONZEPT – HINTERGRUND AUS PRÜFER-PERSPEKTIVE

Maßgeblich für ein wirksames Rechte- und Rollenkonzept ist, dass mehrere Nutzer, die die gleichen Aufgaben und damit die gleiche Rolle im Unternehmen haben, die **gleichen Berechtigungen** bekommen. Statt für jeden Nutzer die Berechtigungen erneut zu definieren, erhalten die Rollen die Berechtigungen. Die Nutzer werden dann den Rollen zugeordnet.

Entscheidend ist die Berechtigungen auf **Widersprüche** zu **überprüfen**. Das gilt besonders, wenn Nutzer verschiedene Rollen gleichzeitig ausüben.

Verschiedene Zugriffsrechte aufgliedern: Bei den Zugriffsrechten reicht die Antwort „Zugriff erlaubt oder nicht“ nicht aus. Für ein revisionssicheres Konzept muss definiert sein, ob ein Anwender nur eine Information lesen darf, ob ein Gerät Daten als Kopie vorhalten oder ob eine Applikation bestimmte Daten löschen darf.

Anforderungen des IDW RS FAIT 1* an die Sicherheit von IT-Systemen im Rahmen der Buchführung

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Autorisierung
- Authentizität
- Verbindlichkeit

Diese Anforderungen sind nur dann zu gewährleisten, wenn eine tatsächlich rollenbezogene Nutzer- und Rechteverwaltung sichergestellt ist.

* IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie

AUSWAHL DES GEEIGNETEN RECHTSGRUNDES

Art. 6 DSGVO

Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a. Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

b. die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

c. die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;

d. die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;

e. die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

f. die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

è **Prüfung, ob *andere* Rechtsgründe als die Einwilligung infrage kommen, ist immer zu empfehlen.**

è **Anwendung des Rechtsgrundes f. „berechtigtes Interesse“ verlangt eine Interessenabwägung.**

VERARBEITUNGEN, DIE OHNE EINWILLIGUNG MÖGLICH SIND

Wofür wird keine datenschutzrechtliche Einwilligung vom Patienten benötigt?

- Bei regulärer Behandlung des Patienten (auch einschl. Einschaltung eines externen Labors)
- Datenübermittlung an Krankenkassen
- Datenübermittlung an Versorgungsämter
- Datenverarbeitung im Zusammenhang mit Krebsregistern
- Datenverarbeitung in krankenhauseigenen Laboren oder auf anderen Stationen.
- Behandlung des Patienten durch mehrere Ärzte oder Konsil

Aussagen des BayLfD zu diesem Thema:

Dürfen im Zusammenhang mit der stationären Versorgung Patientenunterlagen beim Hausarzt/behandelnden Arzt auch dann angefordert oder an diesen übermittelt werden, wenn der Patient aufgrund seines Zustandes **nicht** in der Lage ist, seine Einwilligung hierzu zu erklären?

Die Übermittlung von Patientendaten durch ein Krankenhaus an Dritte ist insbesondere **zulässig** im Rahmen des **Behandlungsverhältnisses** oder dessen verwaltungsmäßiger Abwicklung oder wenn eine Rechtsvorschrift die Übermittlung erlaubt. Informationen, etwa durch den vorbehandelnden (Haus)arzt) sind zulässig, wobei der Erforderlichkeitsprüfung erhebliches Gewicht beizumessen ist.

ABGRENZUNG DER AUFTRAGSVERARBEITUNG

Auftragsverarbeitung im **datenschutzrechtlichen Sinne** liegt nur in Fällen vor, in denen eine **Stelle** von einer **anderen Stelle** im Schwerpunkt mit der **Verarbeitung personenbezogener Daten beauftragt wird („Fachleistung“).**

Die Beauftragung mit fachlichen Dienstleistungen anderer Art, d.h., mit Dienstleistungen, bei denen nicht die Datenverarbeitung im Vordergrund steht bzw. bei denen die Datenverarbeitung nicht zumindest einen wichtigen (Kern-)Bestandteil ausmacht, stellt keine Auftragsverarbeitung im datenschutzrechtlichen Sinne dar.

AUFTRAGSVERARBEITUNG im Sinne von Art. 4 Nr. 8 DS-GVO ist z. B. regelmäßig:

- DV-technische Arbeiten für die Lohn- und Gehaltsabrechnung oder die Finanzbuchhaltung durch Rechenzentren,
- Outsourcing personenbezogener Datenverarbeitung im Rahmen von Cloud-Computing, ohne dass ein inhaltlicher Datenzugriff des Cloud-Betreibers erforderlich ist,
- Sicherheitsdienste, die an der Pforte Besucher- und Anliefererdaten erheben

KEINE AUFTRAGSVERARBEITUNG im Sinne von Art. 4 Nr. 8 DS-GVO (sondern eigene Verantwortlichkeit) ist z. B. regelmäßig:

- Tätigkeiten der Berufsgeheimnisträger (Steuerberater, Rechtsanwälte, externe Betriebsärzte, Wirtschaftsprüfer),
- Labore, Materiallabore usw. (Materialuntersuchung im Auftrag).
- Postdienste für den Brief- oder Paketttransport

TYPISCHE PRAXISPROBLEME BEI DER AUFTRAGSVERARBEITUNG

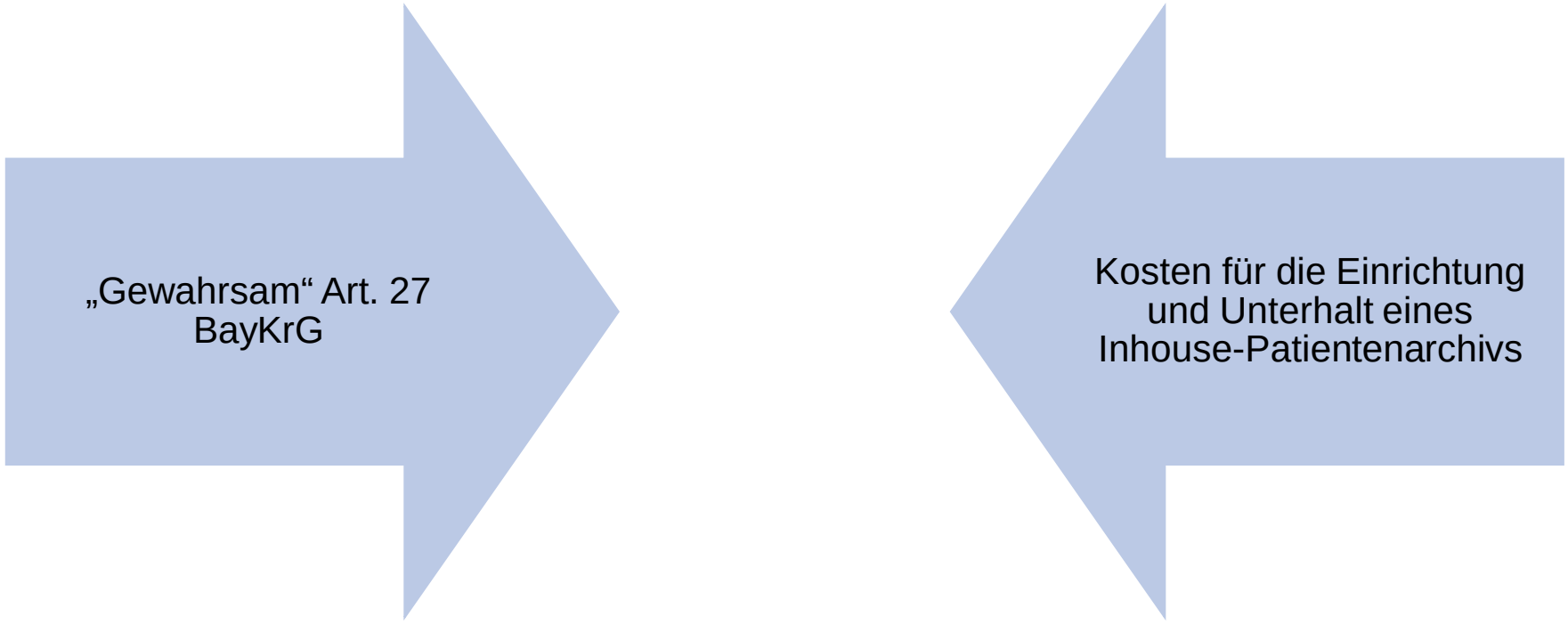
Häufige praktische Probleme:

- Inaktuelle Informationen über die Verträge im Vertragsmanagement
- Relevante Verträge sind im Vertragsmanagement überhaupt nicht erfasst
- Relevante Verträge sind durch einfache Kombination „Angebot“ und „Annahme“ zustande gekommen und werden von den jeweiligen intern Verantwortlichen nicht als Verträge wahrgenommen, daher auch nicht im Vertragsmanagement eingetragen

Folge: Zuverlässige Liste der Vertragsbeziehungen, für die zumindest mittelfristig eine AV-Vereinbarung angestrebt werden sollte, fehlt.

PATIENTENAKTENARCHIV UND DER GEWAHRSAMSBEGRIFF DES BAYKRG

- Anforderung an das Patientenaktenarchiv: Bereitstellung einer elektronischen und hoch verfügbaren Patientenakte zur Sicherstellung der medizinisch erforderlichen Diagnostik und Behandlung der Patienten
- Nebenbedingung: Kosteneffizienz – Wirtschaftlichkeitsgebot
- Ggf. wirtschaftliche Möglichkeiten außerhalb des Krankenhauses denkbar
- Jedoch Herausforderung dabei: Gewahrsamsbegriff im BayKrG



PATIENTENAKTENARCHIV NICHT IM HAUS: DENKBARE LÖSUNG

Substitution eines Dienstleistungsverhältnisses durch eine Auslagerung, bei der der Gewahrsam erhalten bleibt

Kombination aus:

- Dienstleistungsvertrag
- Vereinbarung zur Auftragsverarbeitung
- Arbeitnehmerüberlassungsvertrag
- Mietvertrag

IDENTIFIKATION DER VERARBEITUNGS-TÄTIGKEITEN, FÜR DIE EINE DATENSCHUTZ-FOLGEABSCHÄTZUNG ERFORDERLICH IST

DATENSCHUTZ FOLGEABSCHÄTZUNG

Art. 35 Abs. 1 Satz 1: Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung **voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen** zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch.

Erwägungsgrund 91

Die Verarbeitung personenbezogener Daten sollte **nicht** als umfangreich gelten, wenn die Verarbeitung personenbezogene Daten von Patienten oder von Mandanten betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes oder Rechtsanwalt erfolgt. In diesen Fällen sollte eine **Datenschutz-Folgenabschätzung** nicht zwingend vorgeschrieben sein.

RISIKOPERSPEKTIVE DES BETROFFENEN

Art. 29-Datenschutzgruppe: Kriterien, die bei der Frage nach der Notwendigkeit einer DSFA berücksichtigt werden sollten. Je mehr dieser Kriterien gleichzeitig erfüllt sind, umso wahrscheinlicher ist es, dass ein hohes Risiko für die Rechte und Freiheiten der Betroffenen gegeben ist:

1. Evaluierung oder Scoring, inklusive Profilbildung und Vorhersagen
2. Automatisierte Entscheidungen mit rechtlicher oder ähnlich beeinträchtigender Wirkung
3. Systematische Beobachtung
4. **Sensible Daten**
5. **In großem Umfang verarbeitete Daten**
6. Datensätze, die abgeglichen oder kombiniert wurden
7. **Daten, die verletzliche Datensubjekte betreffen**
8. Innovative Nutzung oder Verwendung von technologischen und organisatorischen Lösungen
9. Datenübermittlung in Drittstaaten außerhalb der EU
10. Datenverarbeitungen, die den Betroffenen davon abhalten, ein Recht geltend zu machen oder einen Dienst oder Vertrag zu nutzen

BLACKLIST: WANN EINE DSFA IN JEDEM FALL ERFORDERLICH IST

Maßgebliche Beschreibung der Verarbeitungstätigkeit	Kommentar / Hinweis
Umfangreiche Verarbeitung von Daten, die dem Sozial-, einem Berufs- oder besonderen Amtsgeheimnis unterliegen, auch wenn es sich nicht um Daten gemäß Art. 9 Abs. 1 und 10 DS-GVO handelt.	
Automatisierte Auswertung von Video- oder Audio-Aufnahmen zur Bewertung der Persönlichkeit der Betroffenen	Videoüberwachung macht DSFA erforderlich.
Verarbeitung von umfangreichen personenbezogenen Daten über das Verhalten von Beschäftigten, die zur Bewertung ihrer Arbeitstätigkeit derart eingesetzt werden können, dass sich Rechtsfolgen für die Betroffenen ergeben oder diese Betroffenen in anderer Weise erheblich beeinträchtigt werden	Erläuterung der DSK: Geolokalisierung von Beschäftigten fällt hierunter. Ggf. bedeutsam für Pflegedienste und entsprechende Tools innerhalb der eingesetzten Dienstplanungssoftware

Beispiele aus der Blacklist der DSK

https://www.lda.bayern.de/media/dsfa_muss_liste_dsk_de.pdf

BEISPIEL VIDEOÜBERWACHUNG

Bevor eine Videoüberwachung installiert wird, ist zu konkretisieren, welches Ziel damit erreicht werden soll. Soweit die Videoüberwachung den gesetzlichen Vorgaben entspricht, kann sie durch eine datenschutzrechtskonforme Betriebsvereinbarung näher geregelt werden.

CHECKLISTE:

- Welche Bereiche sollen überwacht werden?
- Wurde der Zweck der Videoüberwachung schriftlich festgelegt?
- Warum ist die Videoüberwachung das mildeste gleich wirksame Mittel, um den Zweck zu erreichen?
- Sofern aufgezeichnet wird, wann werden die Aufnahmen gelöscht?
- Wurde „je Kamera“ abgewogen bzw. argumentiert?

DATENSCHUTZ-FOLGEABSCHÄTZUNG: INHALT

Art. 35 Abs. 7

DIE FOLGEABSCHÄTZUNG ENTHÄLT FOLGENDES:

a. eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;

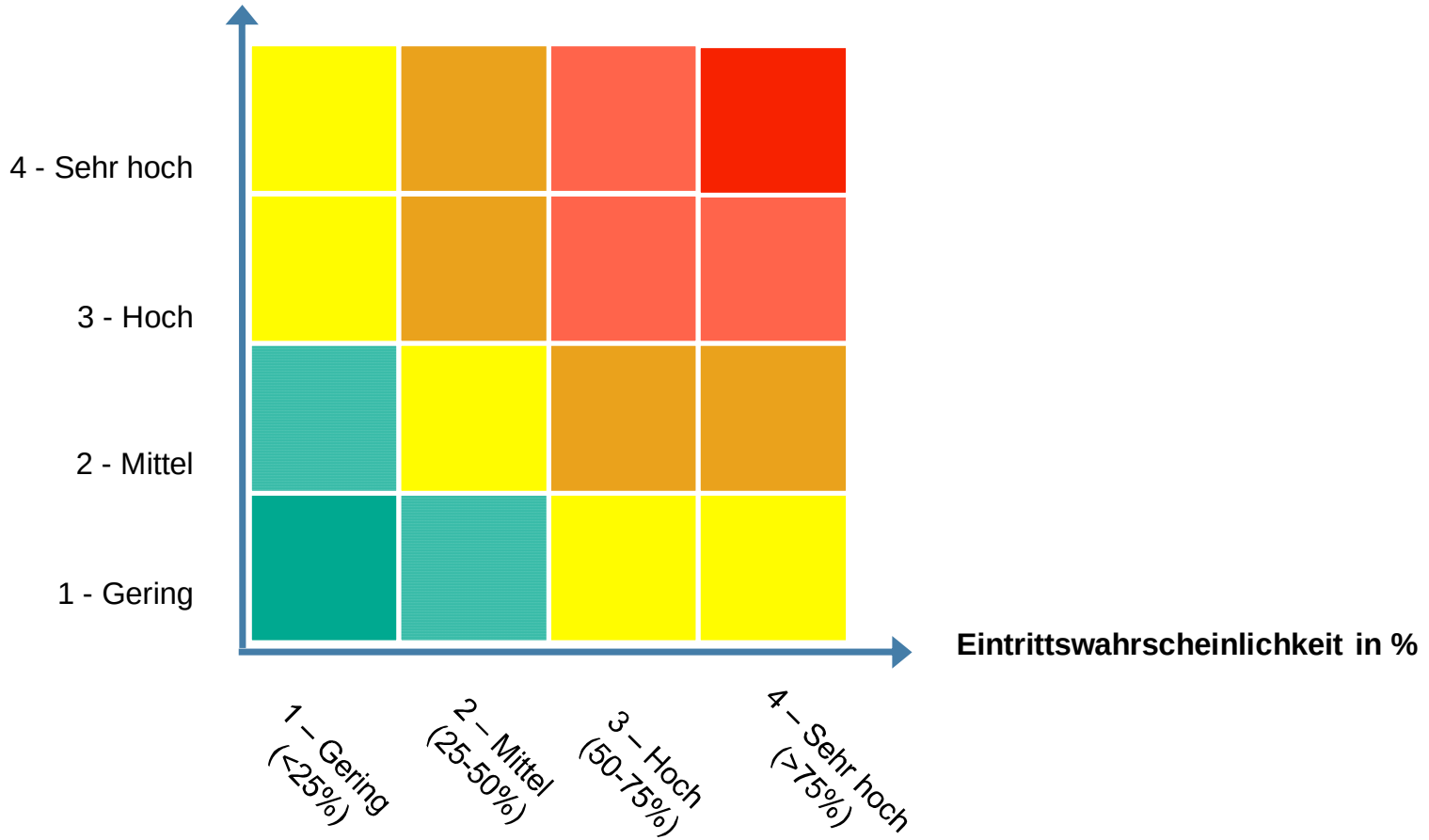
b. eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;

c. eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und

d. die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

RISK-MAP: BEISPIELHAFTER AUFBAU

RISIKOTRAGWEITE / SCHADENSWIRKUNG



STOLPERFALLEN

AB WANN BESTEHEN RECHTSVERSTÖßE?

Der Verantwortliche wird im Fall einer Beschwerde oder eines Verstoßes seiner Rechenschaftspflicht nach Art. Abs. 2 DSGVO faktisch nur dann nachkommen können, wenn er ein dokumentiertes, für den Außenstehenden nachvollziehbares Datenschutzmanagementsystem eingerichtet hat. Dies umfasst mindestens:

1. Nachweis über die rechtswirksame Bestellung des **betrieblichen Datenschutzbeauftragten** und seiner Tätigkeit (= Tätigkeitsbericht)
2. Nachweis angemessener **technischer und organisatorischer Maßnahmen** nach dem aktuellen Stand der Technik
3. **Verzeichnis der Verarbeitungstätigkeiten** einschl. des Nachweises, welchen Zweck die Tätigkeiten jeweils erfüllen und auf welcher Rechtsgrundlage sie erfolgen, dabei auch Nachweis der Datensparsamkeit und Nachweis der Berücksichtigung der besonders sensiblen Daten nach Art. 9 DSGVO
4. Nachweis, dass die **Auskunfts- und Löschungsrechte der Betroffenen** umgesetzt sind (= Prozessbeschreibungen, Anweisungen)
5. Nachweis darüber , dass evtl. **Datenschutzverstöße identifiziert** werden, fristgerecht bewertet werden und bei Vorliegen der Voraussetzungen fristgerecht an die zuständige Aufsichtsbehörde gemeldet werden
6. Nachweis, dass **Mitarbeiter zum Datenschutz verpflichtet** und dass sie **unterwiesen** worden sind und dass relevante Anweisungen für die Mitarbeiter auffindbar und einsehbar sind (Klausel in Arbeitsverträgen, Anweisung Datenschutz, Schulung, Nachweis der Teilnahme der Mitarbeiter)
7. Nachweis der notwendigen Vereinbarungen zur **Auftragsverarbeitung** (Voraussetzung: **aussagefähiges Vertragsmanagement**)
8. Nachweis, dass die wichtigsten Datenschutzrisiken aus Betroffenensicht ermittelt wurden (= **Inventur der Datenschutzrisiken**) und dass die dafür erforderlichen **Datenschutzfolgenabschätzungen** durchgeführt wurden sowie dass ein gesichertes Verfahren zur Durchführung der DSFA eingerichtet ist (= Prozessbeschreibung liegt vor)
9. Nachweis, dass für die Datenweitergaben, für die **Einwilligungserklärungen** erforderlich sind diese systematisch eingeholt werden und dass Mitarbeiter schnell prüfen können, ob die betreffende Einwilligung tatsächlich vorliegt
10. Nachweis, dass ein **Löschkonzept** erstellt wurde und umgesetzt wird

DATENPANNE: WANN BESTEHT DIE MELDEPFLICHT?

Nach Art. 33 ist ein Unternehmen grundsätzlich verpflichtet, eine Verletzung des Schutzes personenbezogener Daten an die zuständige Aufsichtsbehörde zu melden, möglichst binnen 72 Stunden nach Bekanntwerden. Eine **Meldung** kann ausnahmsweise **unterbleiben**, wenn die Datenschutzverletzung nicht zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führt.

Ein Risiko – und damit eine Meldepflicht – besteht nach Erwägungsgrund 75 der DS-GVO immer bei solchen Verarbeitungen, die

- zu physischem, materiellen oder immateriellen Schaden, Diskriminierung, Identitätsdiebstahl/-betrug, finanziellem Verlust, Rufschädigung, Vertraulichkeitsverlust von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, unbefugter Aufhebung der Pseudonymisierung, erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen können,
- betroffene Personen um Rechte und Freiheiten bringt oder diese an der Kontrolle personenbezogener Daten hindert,
- die rassische oder ethnische Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, Gesundheitsdaten, Angaben zum Sexualleben oder strafrechtliche Verurteilungen betreffen

LÖSCHPFLICHT

- Die **Löschpflicht** ergibt sich aus **Art. 5 Abs. 3 lit. e).** Sie beginnt mit dem Ende der gesetzlichen Aufbewahrungspflicht. Für eine Speicherung, die über gesetzliche Aufbewahrungspflichten hinaus geht, muss der Verantwortliche auf Anforderung in der Lage sein, seine eigenen berechtigten Interessen nachzuweisen und dabei darzulegen, warum diese den Schutzbedarf der personenbezogenen Daten überwiegen.
- Außerdem entsteht eine Löschpflicht nach **Art. 17 DSGVO** dann, wenn die betroffene Person dies verlangt, sie eine zuvor abgegebene Einwilligung widerruft oder Widerspruch gegen die weitere Verarbeitung ihrer Daten einlegt

Praxisprobleme:

1. Identifikation und Selektion der löschpflichtigen Daten

2. Die einzelnen IT-Systeme bieten oft (noch) keine Löschmöglichkeit

Lösungsansatz:

- Aufbewahrungspflichten zu den einzelnen Datenkategorien ermitteln und dokumentieren
- Elektronische Speicherung: Softwarehersteller zur Lösung dieses Problems ansprechen. Korrespondenz dazu rechtssicher dokumentieren.
- Papierförmige Speicherung: Archivierungssysteme auf Sortierung „nach Löschjahr“ umstellen.

LÖSCHKONZEPT

Prozess zur Sammlung, Entsorgung/Vernichtung bzw. Löschung von Datenträgern festlegen und schriftlich dokumentieren

- Die Beschreibung muss Regelungen und Verfahren zur sicheren Sammlung bzw. Lagerung sowie Weitergabe inklusive des Transportwegs zur Vernichtung des Datenträgers beinhalten.
- Der Prozess muss datenschutzgerechte Löschverfahren beinhalten.
- Die Vernichtung der Datenträger muss für Dritte (z.B. Aufsichtsbehörden oder Auditoren) nachvollziehbar sein
- Vorgehen zu Vernichtung **DIN 6639947**
- Anregung zur Erstellung eines Löschkonzepts **DIN 6639848**

MITARBEITER-UNTERRICHTUNGSPFLICHT

- Nahezu alle Mitarbeiter in Pflegeeinrichtungen, Pflegediensten und Krankenhäusern kommen mit personenbezogenen Daten der Bewohner, Klienten, und Patienten in Berührung
- Gesetzliche Vertreter sind dafür verantwortlich, Maßnahmen zu ergreifen, um das rechtskonforme Verhalten der Organisation zu gewährleisten. Anderenfalls ggf. Verdacht auf ein betriebliches **Organisationsverschulden**.
  - **Wichtig:** Die Haftung trifft auch solche gesetzlichen Vertreter, die lediglich ehrenamtlich tätig sind (z.B. ehrenamtliche Vorstände eines e.V.)!
- § 203 StGB stellt die Verletzung von Privatgeheimnissen, die jemandem als Angehörigem eines Heilberufs oder als dessen „mitwirkende Person“ bekannt werden, ausdrücklich unter Strafe.
- Die Mitarbeiterschulung ist als eine **zentrale organisatorische Maßnahme im Katalog der TOM‘s** anzusehen.
- Im Falle einer unterlassenen oder nicht dokumentierten Mitarbeiterschulung in einem Pflegeheim oder in einem Krankenhaus ist daher im Fall eines Datenschutzverstoßes ebenfalls mit einer strafrechtlichen Haftung für die gesetzlichen Vertreter der Einrichtung zu rechnen.
- Deshalb ist es sowohl im Interesse der Einrichtung als auch im Interesse der persönlichen Haftungsvermeidung für die Zielgruppe dringend geboten, eine aktuelle, auf die neue Rechtslage angepasste Datenschutzschulung für alle Mitarbeiter durchzuführen und diese auch auf Ebene des einzelnen Teilnehmers zu dokumentieren.
- Insbesondere ist es unumgänglich, Mitarbeitern die Grundzüge und Ziele des Datenschutzes näher zu bringen und diesen die Möglichkeit zu geben, Problemstellungen und Wichtigkeit des Schutzes personenbezogener Daten auf die eigene Person zu reflektieren.
- Neben der Schulung als solcher ist die **Dokumentation der Schulungsteilnahme wichtig.**

EXTERNE PRÜFUNG DER DATENSCHUTZ-COMPLIANCE

EXTERNE PRÜFUNG DER DATENSCHUTZ-COMPLIANCE

Nachweispflicht eines funktionierendes Datenschutz Compliance Management:

- Die gesetzlichen Vertreter einer Organisation sind dafür verantwortlich, Maßnahmen zu ergreifen, um das rechtskonforme Verhalten der Organisation zu gewährleisten. Anderenfalls besteht der Verdacht auf ein betriebliches Organisationsverschulden
- Wenn trotz aller Maßnahmen einmal etwas schiefläuft und eine Datenpanne geschieht, bietet ein Datenschutzaudit wertvolle Anhaltspunkte nach außen hin dafür, dass dennoch kein Organisationsverschulden vorliegt.
- Die Prüfung des CMS nach dem IDW Prüfungsstandard 980 kann auf bestimmte Unternehmensfunktionen eingeschränkt werden. Deshalb eignet sich der Standard u.a. gut dafür, eine gezielte Prüfung des Datenschutz-Compliance-Managementsystems durchzuführen.
- Bescheinigung der Datenschutz-Compliance in einem abgrenzbaren IT-System: IDW PS 860 als Alternative zum PS 980
- Auf Grund der Ausrichtung des IDW PS 860 für IT-Prüfungen sind Prüfungen nach diesem Standard naturgemäß besonders dafür geeignet, Sicherheit über die Angemessenheit und den Implementierungsstand der notwendigen Schutzmaßnahmen zu erlangen
- Ergebnis der Prüfung: Prüfungsbericht des Wirtschaftsprüfers mit entsprechendem Prüfungsvermerk

IHR ANSPRECHPARTNER

Christoph Naucke
Associate Partner
Betriebswirt (Berufsakademie)
Bankkaufmann
Zertifizierter Compliance Officer
Zertifizierter Datenschutzbeauftragter
Zertifizierter IT Compliance Manager

T +49 911 9193 3628

F +49 911 9193 3679

christoph.naucke@roedl.com

www.roedl.de/assurance-it