Solidaris

Wiesbaden, 21. März 2018

Compliance in Kliniken

Integration der datenschutzrechtlichen Anforderungen an ein Compliance-Management-System

WPin StBin Claudia Dues

RA Alexander Gottwald EMBA

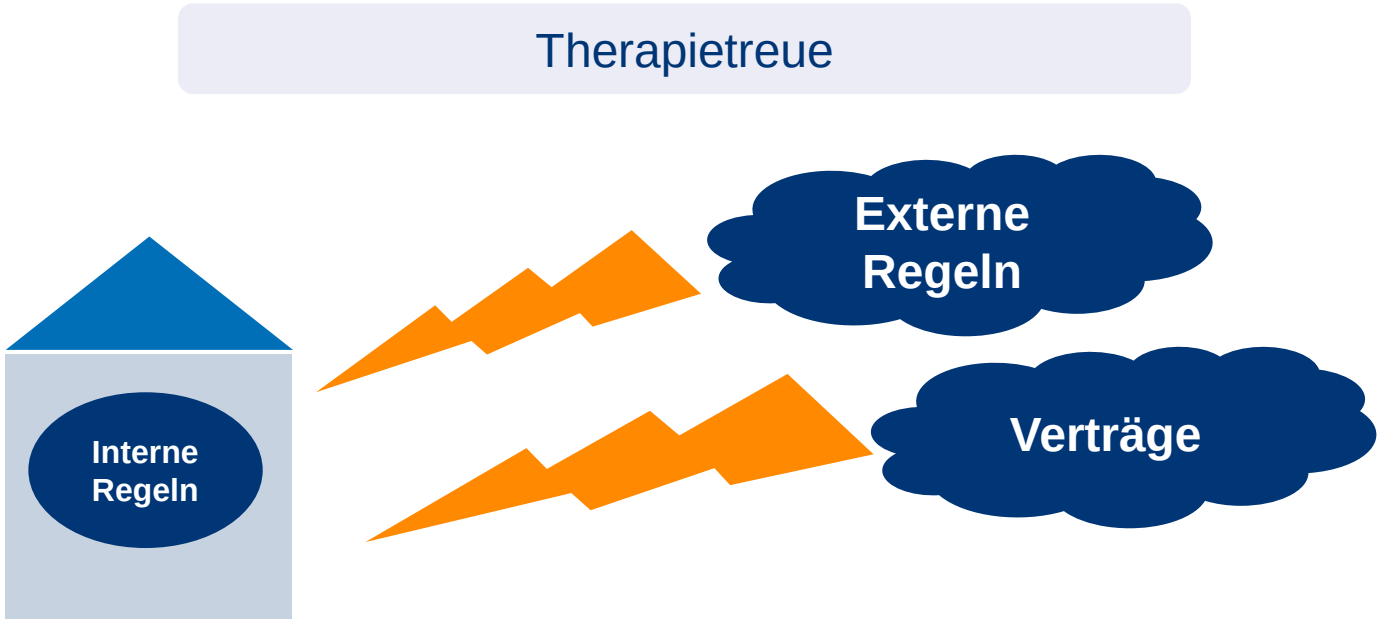
Berlin
Erfurt
Freiburg
Hamburg
Köln
Mainz
München
Münster
Wien (A)
Würzburg

Compliance und Datenschutz ein *„natürliches“ Spannungsfeld“ ein Widerspruch*

- *Neue Datenschutzvorgaben – Compliancetreiber*
- *Datenschutzvorgaben – Leitplanken für Compliance*

„Manchmal muss man sich eben entscheiden – Datenschutz oder Datenverarbeitung“ (im Rahmen eines effektiven CMS) – Nein! – Sondern wirksames Zusammenspiel

Compliance



„Compliance ist die **Summe aller Grundsätze und Maßnahmen**, welche das **ordnungsgemäße Verhalten** der in einem Unternehmen tätigen Organe, Organmitglieder und Mitarbeiter im Hinblick auf **gesetzliche, vertragliche und unternehmenseigene** Regelungen sicherstellen sollen."

Compliance

Rechts-pflicht

- **Eine allgemeine Rechtspflicht zur Implementierung eines Compliance Management Systems besteht nicht**

Notwen-digkeit

- **Die rechtliche Notwendigkeit und der Nutzen eines CMS können aber aus einer Zusammenschau gesetzlicher Pflichten und Rechtsfolgentatbestände (Strafbarkeits- und Ordnungswidrigkeitenregelungen) hergeleitet werden**

Empfeh-lung

- **Neben unterschiedlichen gesetzlichen Regelungen betonen vor allem im Gesundheits- und Sozialwesen Ansätze zur Unternehmensführung und eine Vielzahl von Kodizes das Erfordernis, teilweise auch die Pflicht, ein CMS einzuführen**

…. durch Compliance werden Wertvorstellungen, Moral und Ethik im Unternehmen verankert!
Interne und externe Haftungsrisiken werden reduziert

Compliance – organisatorische Umsetzung

1. Compliance-Kultur
- Grundeinstellung *„tone at the top“ & „walk like you talk“*
- Wertesystem

2. Compliance-Ziele
- Festlegung wesentlicher Ziele
- Eingrenzung wesentlicher Teilbereiche und deren Regeln

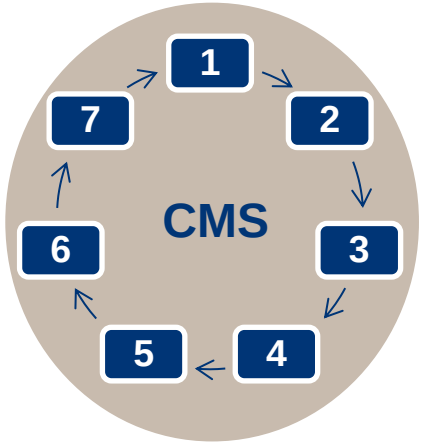
3. Compliance-Risiken
- Identifikation von Risiken
- Beurteilung und Systematisierung der wesentlichen Risiken

4. Compliance-Programm
- Basierend auf den wesentlichen Risiken werden Maßnahmen und Grundsätze abgeleitet
- Prävention und Kontrolle

5. Compliance-Organisation
- Zuweisen von Aufgaben und Verantwortlichkeiten in der Organisation
- Ressourcenplanung

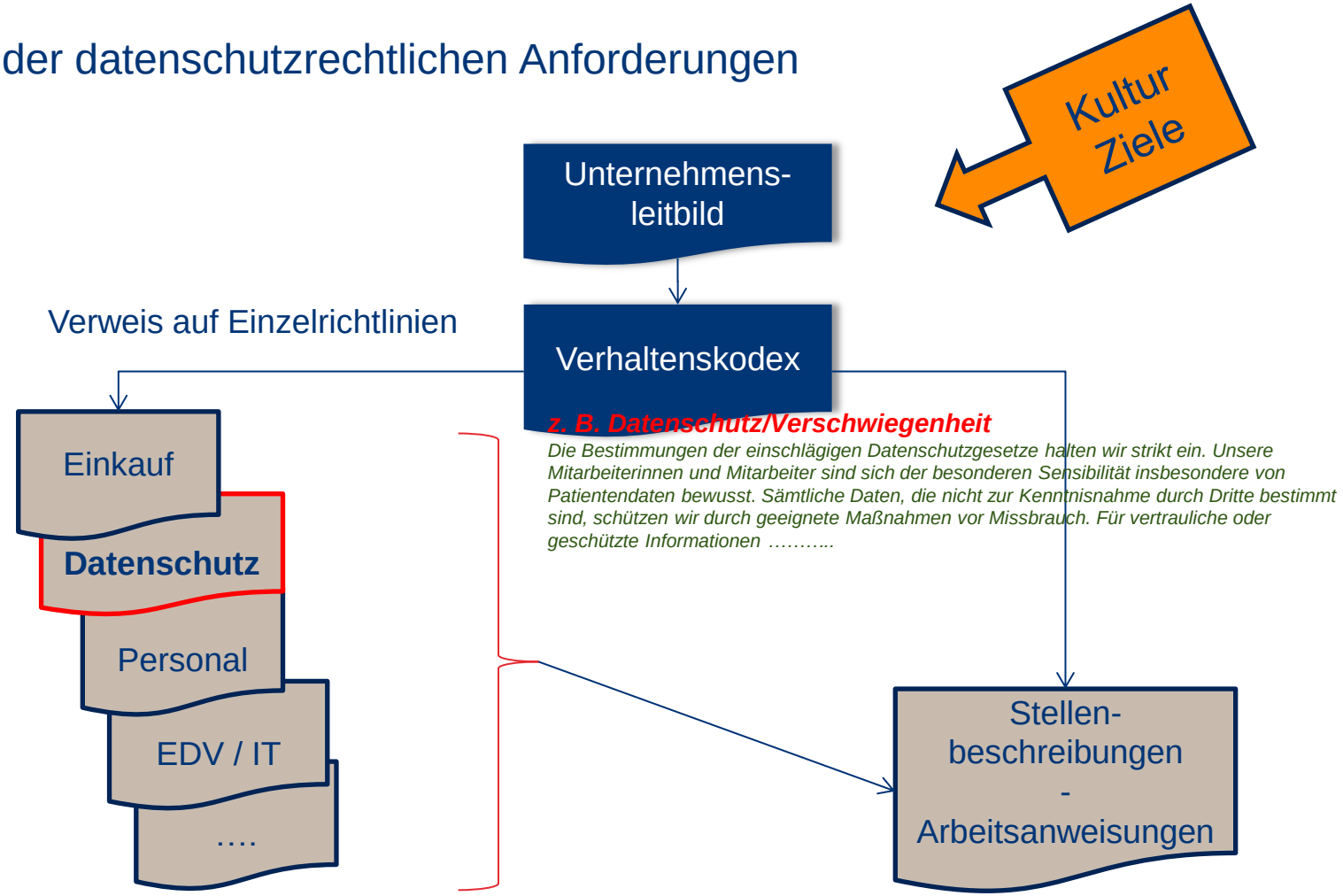
6. Compliance-Kommunikation
- Aktive Information aller Mitarbeiter
- Festlegung von Berichtswegen zur Meldung von Verstößen oder Risiken (Hinweisgeberverfahrens)

7. Compliance-Überwachung/ Verbesserung
- Kontinuierliche Sicherstellung der Angemessenheit und Wirksamkeit
- **Berichterstattung**
- Dokumentation und Fortentwicklung



„Tone of the top“

Integration der datenschutzrechtlichen Anforderungen

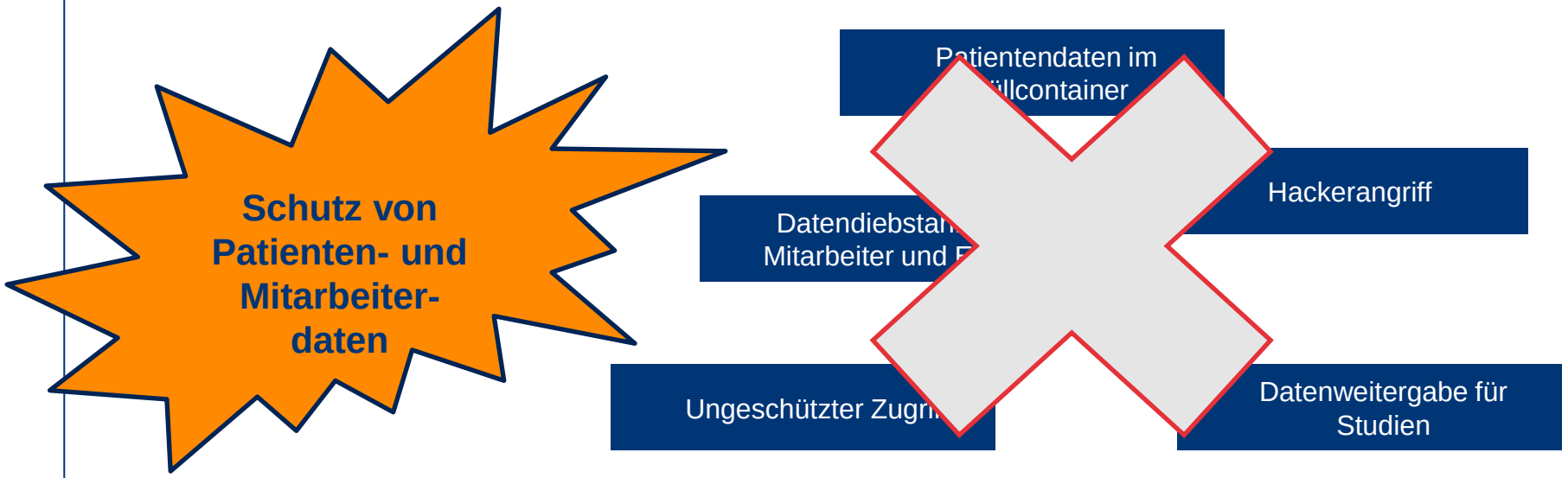


Einzelrichtlinien unter Berücksichtigung der relevanten Regeln und Handlungsanweisungen

Compliance Ziel

Sicherstellung / Einhaltung der Datenschutzregeln ist Teil der Unternehmenskultur

Welche datenschutzrelevanten Vorgaben gibt es und werden diese Vorgaben gesetzeskonform umgesetzt und beachtet?



Compliance Ziel

Sicherstellung / Einhaltung der Datenschutzregeln ist Teil der Unternehmenskultur

- Bei jeder datenschutzrechtlichen Verarbeitungstätigkeit und deren Dokumentation sind folgende Prinzipien zu beachten

	Ermessens-spielraum
Rechtmäßigkeit	✗
Zweckmäßigkeit	✓
Wirtschaftlichkeit	✓

Solidaris

Exkurs

Wesentliche Änderungen durch die Datenschutzreform 2018

Datenschutzreform – Fahrplan in der Gesetzgebung

- 25. Mai 2016 – Verkündung der DS-GVO – Umsetzungsfrist zwei Jahre
- 30. Juni 2017 – Verkündung des nationalen „Anpassungsgesetzes“ der DS-GVO, das modifizierte BDSG
- Reform des kirchlichen Datenschutzes November 2017
  - KDO wird zum KDG – November 2017
  - KDR-OG – Datenschutz der Ordensgemeinschaften – Januar 2018
  - DSG-EKD wird reformiert
  - Umsetzungsfrist weniger sechs Monate
- 24. und 25. Mai 2018 – Regelungen treten in Kraft

Datenschutzreform – Kernthemen

- Gründe für Reform: Massiver Anstieg der Datenverarbeitung und Attacken auf IT-Infrastrukturen – Stärkere Einbindung des Verantwortlichen

- Einführung Dokumentations- und Nachweispflicht durch Rechenschaftspflicht
  ➔ Beweislastumkehr
  - Notwendige Einführung eines Datenschutz-Management-Systems und Integration in ein vorhandenes Compliance-Management-System

- Ausweitung der Rechte des Betroffenen und größere Transparenz der Verarbeitung der Daten ➔ umfangreiche Informations-, Auskunfts- und Benachrichtigungspflichten des Verantwortlichen

- Verlagerung der Verantwortlichkeiten bei der Auftrags(daten)-verarbeitung

Datenschutzreform – Kernthemen

- Aufbau eines Verzeichnisses der Verarbeitungstätigkeiten (VVT)
- Teilweise Verpflichtung zur Benennung eines Datenschutzbeauftragten in kirchlichen Einrichtungen
- Stand der Technik und Risikoorientierung etwa zur Festlegung von erforderlichen „technisch, organisatorischen Maßnahmen“ (TOM)
  z. B. Verschlüsselung von E-Mails, um Vertraulichkeit zu gewährleisten
- Steigerung des Bußgeldrahmens von derzeit bis zu 300.000 EUR auf bis zu 10 - 20 Mio. EUR oder 2 - 4 % des weltweiten Jahresumsatzes; KDG / DSG-EKD auf 500.000 EUR

➔ Datenschutz wird zu einem erheblichen Kosten- und Risikofaktor für Unternehmen

Zulässigkeit der pb-DV

Erwägungsgrund (EG) 40, Art. 6 DS-GVO

- Verbot mit Erlaubnisvorbehalt
  - ➔ Verarbeitung von personenbezogenen Daten ist zunächst erst einmal verboten
  - ➔ **Ausnahmen**
    - ➔ Erlaubnis aus DS-GVO / BDSG 2018 / KDG / DSG-EKD
    - ➔ aus sonstigem Unionsrecht (Sofern die DS-GVO darauf Bezug nimmt)
    - ➔ nach dem Recht der Mitgliedstaaten (Nutzung der Öffnungsklauseln unterstellt)
    - ➔ Einwilligung des Betroffenen

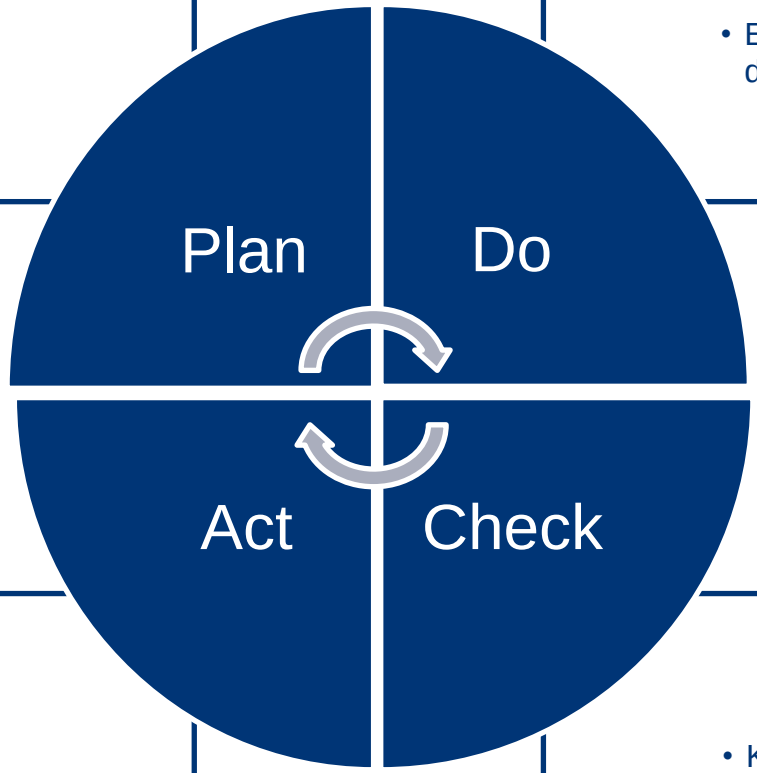
Grundsätze der Verarbeitung

Erwägungsgrund (EG) 40, Art. 5 DS-GVO

Auswirkungen – Aufbau eines DSMS

- Thema (an)erkennen
- Umsetzung planen

- Umsetzung koordinieren
- Ergebnisse dokumentieren



- Verbesserungs-potenzial analysieren

- Kontrolle dokumentieren

Umfang des Datenschutz-Management-System (DSMS)

- Das DSMS umfasst die regelmäßige Kontrolle und Optimierung im Hinblick auf:
  - Risikobewertung und Risikomanagement
  - Verarbeitungsgrundsätze
  - Verarbeitungsverzeichnisse
  - technisch-organisatorischen Maßnahmen
  - Durchführung von Datenschutz-Folgeabschätzungen, Bestellung / Einbindung eines Datenschutzbeauftragten
  - Vertragsmanagement (Auftrags(daten)verarbeitung)
  - Prozesse zur Wahrnehmung der Betroffenenrechte
  - Meldung von Datenschutzverstößen
  - Schulung der Mitarbeiter

Verantwortlichkeiten / Hauptaufgaben

Unternehmens-ebene

Etablierung:
- Datenschutz-Management (DSMS)
- IT-Sicherheits-Management (ISMS)

Abteilungs-ebene

Umsetzung
- Prozessgestaltung (Privacy by design/default)
- Datenschutzfolgeabschätzung
- Dokumentation / Nachweise / Meldepflichten
- Prozesse für Rechte der Betroffenen

IT-Abteilung

Umsetzung:
- Vorgaben des ISMS

Unterstützung:
- Technische Umsetzung der Datenschutzvorgaben in den Prozessen

Datenschutz-beauftragter

Beratung:
- Abstimmung bei „Strategien“ und – vorgegebenen Einzelfällen „Überwachung“
- Umsetzung, risikoorientiert

Umsetzungszyklus

Bestandsaufnahme	Feststellung des Handlungsbedarfs – Frage nach neuen DV? Dokumentation der Bewertung der Ergebnisse
Definition der Datenschutzziele	Leitprinzipien und Richtlinien durch die Geschäftsleitung aktualisieren
Konzeption des DSMS	Umsetzung der Datenschutzziele durch: ▪ Regelung der Verantwortlichkeiten ▪ Erstellung von Richtlinie, Handlungsanweisungen etc. für die Mitarbeiter ▪ Entwicklung von technisch-organisatorischen Maßnahmen
Information	Information und Sensibilisierung der Mitarbeiter
Umsetzung	Umsetzung der Konzeption
Kontrolle / Bericht	Kontrolle / Audit zur Fortentwicklung des Konzepts

Auswirkungen auf betriebliche Organisation

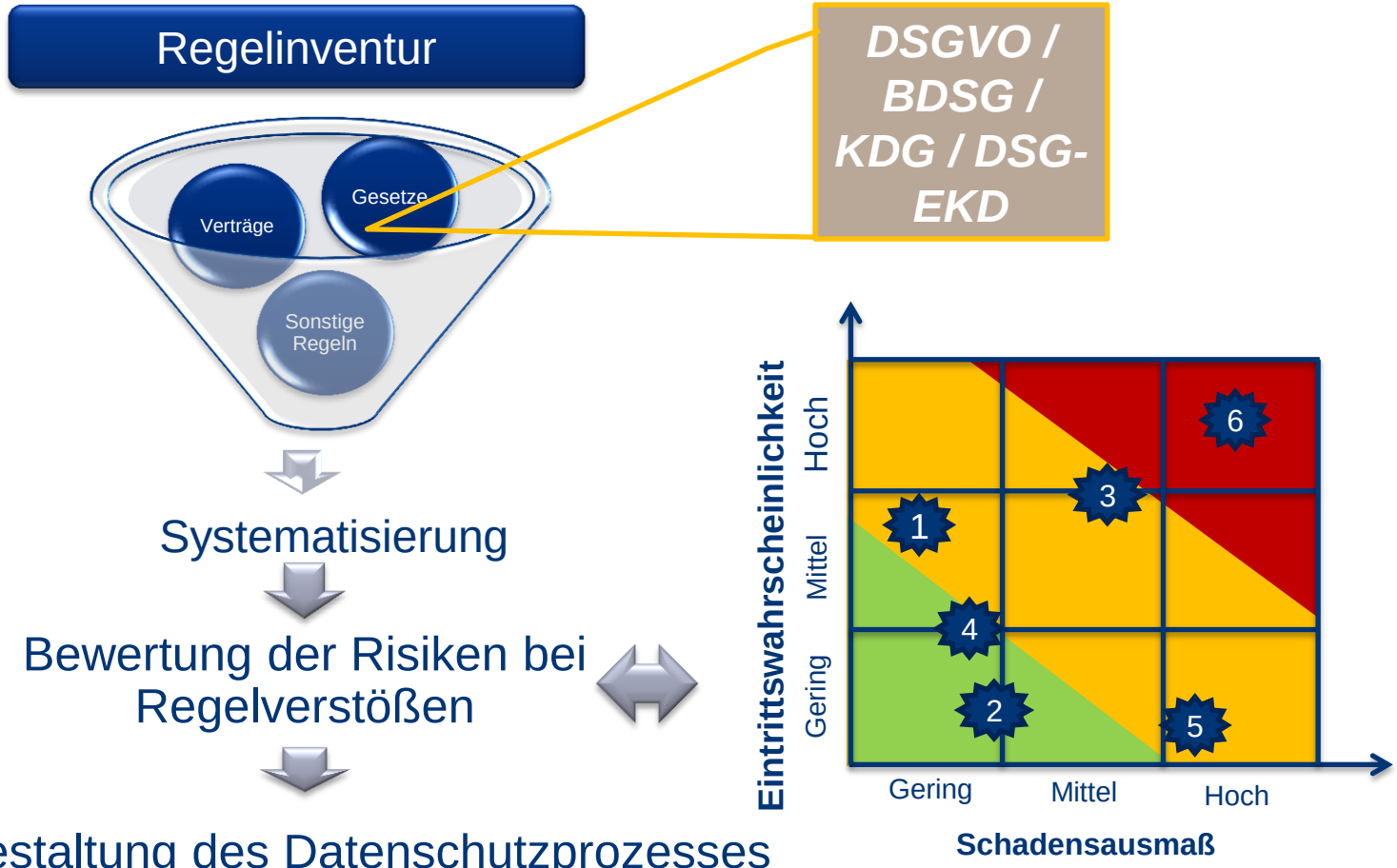
- Erarbeitung einer Konzeption zum Datenschutz
- Anpassung sämtlicher datenschutzrelevanter (IT-)Prozesse
- Rechenschaftspflicht führt zu mehr Dokumentationsaufwand (Exkulpation)
- Stärkere Dokumentation der Datenverarbeitungsprozesse im Unternehmen
- Überarbeitung Datenschutz-(Erweiterung der Informationspflichten) und Einwilligungserklärungen (Verschärfung der formalen Vorgaben)
- Anpassung der Betriebs- und Dienstvereinbarungen Durchführung von zielgruppengerechten Schulungen der Mitarbeiter zu den Neuerungen

Solidaris

Exkurs - Ende

Compliance Risiken

Analyse für den Bereich Datenschutz



Compliance Risiken

Systematisierung – Atlas

Behandlung	Kooperationen	Abrechnung	Einkauf	Technik / Hygiene / Apotheke	Personal	Sonstige
Strukturelle Organisationsmängel / Qualität und Sicherheit von Dienstleistungen	Vorteilnahme und Bestechlichkeit (§§ 331, 332 StGB)	Korrekte Abrechnung ggü. • Krankenkassen, • KV • Privatpatienten • Wahlleistungen	Vergaberecht für öffentliche Fördermittel	Apothekengesetz - ApoG	Diskriminierungsverbot (Gleichstellung, Mobbing, Schwerbehinderte …)	Umgang mit Arbeitsmitteln
Individuelle Behandlungsfehler	Bestechlichkeit und Bestechung im geschäftlichen Verkehr (§ 299 StGB)	Persönl. Leistungserbringung • Wahlärztl. Leistungen • Ermächtigungen • CA-Ambulanzen • MVZ	Interne Vergabe- und Ausschreibungsregeln	Apothekenbetriebsordnung - APBetrO	Arbeitszeitgesetze / Arbeitsschutzgesetze / Mutterschutz	Gemeinnützigkeit iSd. AO / Begünstigungsverbot
Fahrlässige Tötung (§ 222 StGB)	Bestechlichkeit und Bestechung im Gesundheitswesen (§ 299a StGB)	Zuweisungsprämien	Zuwendungen / Geschenke / Bewirtungen	Regelung und Kontrolle des legalen und sicheren Umgangs mit Arznei- und Betäubungsmitteln (AMG, BtMG)	Verhaltenskodex / Grundordnung	Spenden / Sponsoring (eigenes)
Fahrlässige Körperverletzung (§ 229 StGB)	Kooperationen mit Industrie	Honorar, Beleg- und Konsiliarärzte	Preis- und Mengenabsprachen	Medizinproduktegesetz - MPG	Vorteile / Geschenke / Bewirtungen / Einladungen	Schutz von Firmeneigentum
Totschlag (§ 212 StGB)	Kooperationen mit niedergelassenen Ärzten	Regelungen zu Mindestmengen	Unzulässige Rabattgestaltung / Kick-backs	Strahlenschutzverordnung, Röntgenverordnung	Persönliche und finanzielle Unabhängigkeit / Verhalten bei nahestehenden Personen	Kommunikation mit der Öffentlichkeit
Körperverletzung mit Todesfolge (§ 227 StGB)	Drittmittel, Arzneimittel und Studien, Sponsoring, Einladungen/Zuwendungen	Abrechnung mit einem Vermittler ohne den Patienten zu informieren		Interne Hygiene-Richtlinie	Verschwiegenheit / Vertraulichkeit / Umgang mit Betriebsgeheimnissen	Nachhaltigkeit
Embryonenschutzgesetz - ESchG	Kartellrecht / Zusammenschlüsse von Kliniken / Einkaufsverbünde	Umgang mit Bargeldgeschäften		Infektionsschutzgesetz	Schutz der Patienten und Mitarbeiter vor sexuellen oder gewalttätigen Übergriffen durch das Personal (§ 174a StGB) oder Dritten	Brand- und Katastrophenschutz
Datenschutz						

Compliance Risiken

Analyse für den Bereich Datenschutz

- Verletzung der Schweigepflicht von Berufsgeheimnisträgern
- Unzulässige Erhebung / Weitergabe von personenbezogenen Daten
- Verletzung des Briefgeheimnisses
- Verletzung von Geschäfts- und Betriebsgeheimnissen
- Verstoß gegen die Meldepflicht
- Verstoß gegen die Rechte des Betroffenen
- Verstoß gegen die Verarbeitungsgrundsätze
- Verstoß gegen Recht am eigenen Bild
- ……..

Compliance Programm – Prävention und Kontrolle

Strukturierte Analyse und Auswertung von Daten, Prozessen…..Audits

- (Unzulässige) Erhebung / Weitergabe von personenbezogenen Daten
- Aufbewahrung von personenbezogenen Daten
- Vernichtung von personenbezogenen Daten

Entwicklung von Einzelrichtlinien

- Datenschutzrichtlinie
- Datenschutzerklärung/Verschwiegenheitserklärung
- Nutzungsrichtlinien
- Verfahrensanweisungen / Arbeitsanweisungen
- Datenschutzfolgeabschätzungen
- Betriebsvereinbarungen…..

Compliance Programm – Prävention und Kontrolle

... Integration der Datenschutzvorgaben – in den Aufnahmeprozess

- *Erhebung nur solcher Daten, die zur Leistungserbringung bzw. Abrechnung benötigt werden*

Fragestellungen

- Werden in der Aufnahme auch Daten erhoben, die für die obigen Zwecke nicht erforderlich sind
- Werden zusätzliche (nützliche) Daten erhoben, und werden diese entsprechend gekennzeichnet
- An welcher Stelle erhält der Patient Informationen über die Datenverarbeitungen
- Hat der Patient der Weitergabe seiner Daten an Dritte zugestimmt - Funktionsübertragung vs. Auftrags(daten)verarbeitung (aber auch Auskunftserteilung an Angehörige u. a.)

Arbeitsanweisungen

Compliance Programm – Prävention und Kontrolle

- Datenaustausch im Konzern, unter Kliniken, mit Ärzten und mit Dienstleistern

  - Besteht Einwilligung oder ist neue Einwilligung erforderlich?
  - Wer bleibt verantwortlich für die Daten?
  - Funktionsübertragung vs. Auftragsdatenverarbeitung
  - (auch) kein Konzernprivileg nach DS-GVO / KDG / DSG-EKD
  - Auftrags(daten)verarbeitung
    - Welche Verträge bestehen?
    - Verwendung von „Hybriden“ oder Anpassungs- und Ablösungsverträgen

Compliance Programm – Prävention und Kontrolle

... Integration der Datenschutzvorgaben in den Einkaufsprozess

Fragestellungen

- sind (Muster)verträge mit den aktuellsten rechtlichen Vorgaben versehen – Compliance Klausel
  - Musterverträge zur Auftrags(daten)verarbeitung
  - Klauseln zum Datenschutz – Verschwiegenheitserklärung
- Ist die Einhaltung der Datenschutzvorgaben bei dem externen Datenverarbeiter sichergestellt bzw. überprüft (Kodizes, Due Diligence, Selbstauskunft)

Arbeitsanweisungen

Compliance Programm – Prävention und Kontrolle

- „Need-to-Know-Prinzip“
  - Jeder soll nur die Daten kennen, die er für seine Arbeit kennen muss

    ➔ Abschaffung der Gruppenaccounts (Single Sign-On, MFI)
  - Problem: Ärzte und Personal in Nachtschicht besitzen sämtliche Berechtigungen für die Einsicht in Akten für Notfälle – auch künftig kein Problem wegen Notfall-Rechtfertigung
  - ABER: Protokollierung wichtig und stichprobenartige Kontrolle ggf. Notfallberechtigung einführen

- Heranziehung von Vorbehandlungsdaten
  - Widerspruchs- vs. Einwilligungslösung
  - Künftig wohl nur Einwilligung möglich oder Interessenabwägung

Compliance Kommunikation

Aktive Information aller Mitarbeiter und Festlegung von Berichtswegen zur Meldung von Verstößen oder Risiken (Hinweisgeberverfahrens)

- Datenschutzrichtlinie u. a. - Mitarbeiterunterweisung durch Veröffentlichung im Intranet, … Vortrag, … Aushändigung
- Richtlinie zur Sicherstellung und Zusicherung der vertraulichen Behandlung der Identität der Hinweisgeber
- ……

Compliance Organisation / Überwachung – Kontrolle

Zuweisen von Aufgaben und Verantwortlichkeiten in der Organisation – Ressourcenplanung

- Compliance Beauftragter (interne – externe Besetzung)
  - Implementierung / Dokumentation / Weiterentwicklung
  - Sicherstellung der Einhaltung der gesetzlichen und unternehmensinternen Anforderungen - auch bei deren Kontrolle - Meldung von NonCompliance

- Datenschutzbeauftragter (Art. 39 DS-GVO / § 7 BDSG 2018)
  - Unterrichtung und Beratung
  - Überwachung der Einhaltung der DS-GVO sowie der Strategien der Verantwortlichen
  - Zuweisung von Zuständigkeiten
  - Sensibilisierung und Schulung von Mitarbeitern (einschl. Überprüfung)
  - Beratung Datenschutzfolgeabschätzung

Solidaris

Compliance der Datenschutzvorgaben
und
Einhaltung der Datenschutzvorgaben bei der Compliance
kein Widerspruch
sondern
zwei Seiten einer Medaille

„Ausdruck der Unternehmenskultur und Aushängeschild“

Vielen Dank für Ihre Aufmerksamkeit!

Claudia Dues
Wirtschaftsprüferin / Steuerberaterin
Tel. 02203 | 8997-143
E-Mail: c.dues@solidaris.de

Alexander Gottwald, EMBA
Rechtsanwalt
Externer Datenschutzbeauftragter (GDDcert. EU)
Tel. 0251 I 48261-173
E-Mail: a.gottwald@solidaris.de