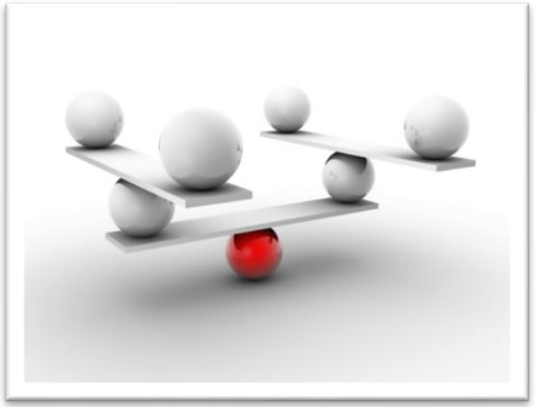
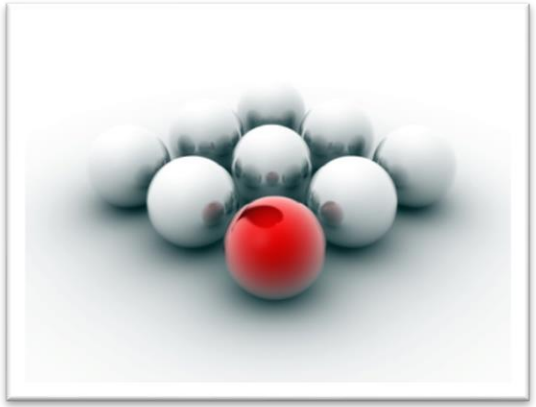
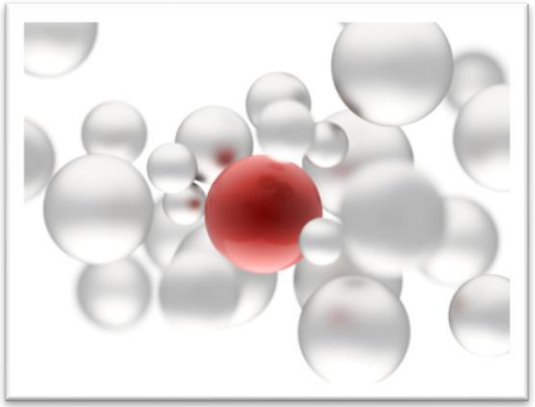
CETUS
Health · IT · Leadership







IT-Sicherheitsmanager für medizinische IT-Netzwerke

Risiken ohne Nebenwirkungen.

Agenda

Tag 1

- ✓ 5.1. Rechtliche Grundlagen
  - Rechtliche Grundlagen 1: Klinisch
  - Rechtliche Grundlagen 2: Kaufmännisch
- ✓ 5.2. Normen & Managementsysteme

Tag 2

- ✓ 5.3. Risikoanalyse

Rechtliche Grundlagen 1: Klinisch

- ✓ Gesetz über Medizinprodukte (Medizinproduktegesetz - MPG)
- ✓ Verordnung über das Errichten, Betreiben und Anwenden von Medizinprodukten (MPBetreibV)
- ✓ Verordnung (EU) 2017/745 über Medizinprodukte (MDR)
- ✓ Verordnung über den Schutz vor Schäden durch Röntgenstrahlen (RöV)
- ✓ Richtlinien und Regelungen des Gemeinsamen Bundesausschusses (G-BA Richtlinien)
- ✓ Sozialgesetzbuch (SGB) Buch (1-12)

Gesetz über Medizinprodukte (Medizinproduktegesetz - MPG)

§ 2 Anwendungsbereich des Gesetzes

(1) Dieses Gesetz gilt für Medizinprodukte und deren Zubehör. Zubehör wird als eigenständiges Medizinprodukt behandelt.

(2) Dieses Gesetz gilt auch für das Anwenden, Betreiben und Instandhalten von Produkten, die nicht als Medizinprodukte in Verkehr gebracht wurden, aber mit der Zweckbestimmung eines Medizinproduktes im Sinne der Anlagen 1 und 2 der Medizinprodukte-Betreiberverordnung eingesetzt werden. Sie gelten als Medizinprodukte im Sinne dieses Gesetzes. …

(4) Die Vorschriften des Atomgesetzes, der Strahlenschutzverordnung, der Röntgenverordnung und des Strahlenschutzvorsorgegesetzes, … sowie die Rechtsvorschriften über Geheimhaltung und Datenschutz bleiben unberührt.

§ 4 Verbote zum Schutz von Patienten, Anwendern und Dritten

(1) Es ist verboten, Medizinprodukte in den Verkehr zu bringen, zu errichten, in Betrieb zu nehmen, zu betreiben oder anzuwenden, wenn

1. der begründete Verdacht besteht, dass sie die Sicherheit und die Gesundheit der Patienten, der Anwender oder Dritter bei sachgemäßer Anwendung, Instandhaltung und ihrer Zweckbestimmung entsprechender Verwendung über ein nach den Erkenntnissen der medizinischen Wissenschaften vertretbares Maß hinausgehend unmittelbar oder mittelbar gefährden oder
2. das Datum abgelaufen ist, bis zu dem eine gefahrlose Anwendung nachweislich möglich ist.

§ 6 Voraussetzungen für das Inverkehrbringen und die Inbetriebnahme

(1) Medizinprodukte, mit Ausnahme von Sonderanfertigungen, Medizinprodukten aus Eigenherstellung, Medizinprodukten gemäß § 11 Abs. 1 sowie Medizinprodukten, die zur klinischen Prüfung oder In-vitroDiagnostika, die für Leistungsbewertungszwecke bestimmt sind, dürfen in Deutschland nur in den Verkehr gebracht oder in Betrieb genommen werden, wenn sie mit einer CE-Kennzeichnung nach Maßgabe des Absatzes 2 Satz 1 und des Absatzes 3 Satz 1 versehen sind. Über die Beschaffenheitsanforderungen hinausgehende Bestimmungen, die das Betreiben oder das Anwenden von Medizinprodukten betreffen, bleiben unberührt

§ 19 Klinische Bewertung, Leistungsbewertung

(1) Die Eignung von Medizinprodukten für den vorgesehenen Verwendungszweck ist durch eine klinische Bewertung anhand von klinischen Daten nach § 3 Nummer 25 zu belegen, soweit nicht in begründeten Ausnahmefällen andere Daten ausreichend sind. Die klinische Bewertung schließt die Beurteilung von unerwünschten Wirkungen sowie die Annehmbarkeit des in den Grundlegenden Anforderungen der Richtlinien 90/385/EWG und 93/42/EWG genannten Nutzen-/Risiko-Verhältnisses ein. Die klinische Bewertung muss gemäß einem definierten und methodisch einwandfreien Verfahren erfolgen und gegebenenfalls einschlägige harmonisierte Normen berücksichtigen.

§ 20 Allgemeine Voraussetzungen zur klinischen Prüfung

(1) Mit der klinischen Prüfung eines Medizinproduktes darf in Deutschland erst begonnen werden, wenn die zuständige EthikKommission diese nach Maßgabe des § 22 zustimmend bewertet und die zuständige Bundesoberbehörde diese nach Maßgabe des § 22a genehmigt hat. … Die klinische Prüfung eines Medizinproduktes darf bei Menschen nur durchgeführt werden, wenn und solange

1. die Risiken, die mit ihr für die Person verbunden sind, bei der sie durchgeführt werden soll, gemessen an der voraussichtlichen Bedeutung des Medizinproduktes für die Heilkunde ärztlich vertretbar sind, 1a. ein Sponsor oder ein Vertreter des Sponsors vorhanden ist, der seinen Sitz in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum hat,

MPG

2. die Person, bei der sie durchgeführt werden soll, ihre Einwilligung hierzu erteilt hat, nachdem sie durch einen Arzt, bei für die Zahnheilkunde bestimmten Medizinprodukten auch durch einen Zahnarzt, über Wesen, Bedeutung und Tragweite der klinischen Prüfung aufgeklärt worden ist und mit dieser Einwilligung zugleich erklärt, dass sie mit der im Rahmen der klinischen Prüfung erfolgenden Aufzeichnung von Gesundheitsdaten und mit der Einsichtnahme zu Prüfungszwecken durch Beauftragte des Auftraggebers oder der zuständigen Behörde einverstanden ist,

…

§ 20 Allgemeine Voraussetzungen zur klinischen Prüfung

(2) Eine Einwilligung nach Absatz 1 Nr. 2 ist nur wirksam, wenn die Person, die sie abgibt, 1. geschäftsfähig und in der Lage ist, .., Risiken, … Tragweite der klinischen Prüfung einzusehen und ihren Willen hiernach zu bestimmen, 2. die Einwilligung selbst und schriftlich erteilt hat. Eine Einwilligung kann jederzeit widerrufen werden

§ 21 Besondere Voraussetzungen zur klinischen Prüfung (Einwilligungsvoraussetzungen gelten analog auch für gesetzliche Vertreter)

(4) Ist die Genehmigung einer klinischen Prüfung zurückgenommen oder widerrufen oder ruht sie, so darf die klinische Prüfung nicht fortgesetzt werden.

MPG

5. soweit erforderlich, eine dem jeweiligen Stand der wissenschaftlichen Erkenntnisse entsprechende biologische Sicherheitsprüfung oder sonstige für die vorgesehene Zweckbestimmung des Medizinproduktes erforderliche Prüfung durchgeführt worden ist.
6. soweit erforderlich, die sicherheitstechnische Unbedenklichkeit für die Anwendung des Medizinproduktes unter Berücksichtigung des Standes der Technik sowie der Arbeitsschutz- und Unfallverhütungsvorschriften nachgewiesen wird,

…

§ 30 Sicherheitsbeauftragter für Medizinprodukte

(1) Wer als Verantwortlicher nach § 5 Satz 1 und 2 seinen Sitz in Deutschland hat, hat unverzüglich nach Aufnahme der Tätigkeit eine Person mit der zur Ausübung ihrer Tätigkeit erforderlichen Sachkenntnis und der erforderlichen Zuverlässigkeit als Sicherheitsbeauftragten für Medizinprodukte zu bestimmen.

(2) Der Verantwortliche muss den Sicherheitsbeauftragten der zuständigen Behörde anzeigen, (auch Wechsel)

(3) Der Nachweis der erforderlichen Sachkenntnis als Sicherheitsbeauftragter für Medizinprodukte … muss erbracht werden.

(4) Der Sicherheitsbeauftragte für Medizinprodukte hat … Meldungen über Risiken bei Medizinprodukten zu sammeln, zu bewerten und… Maßnahmen zu koordinieren. Er ist für die Erfüllung von Anzeigepflichten verantwortlich, soweit sie Medizinprodukterisiken betreffen.

§ 40 Strafvorschriften (gekürzt)

(1) Freiheitsstrafe bis zu drei Jahren mit 1. entgegen § 4 Abs. 1 Nr. 1 ein Medizinprodukt in den Verkehr bringt, errichtet, in Betrieb nimmt, betreibt oder anwendet,

2. entgegen § 6 Abs. 1 Satz 1 analog entgegen Strahlenschutzverordnung oder Röntgenverordnung

3. entgegen § 6 Abs. 2 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 37 Abs. 1 ein Medizinprodukt, … mit der CE-Kennzeichnung versieht oder

4. entgegen § 14 Satz 2 ein Medizinprodukt betreibt oder anwendet. (2) Der Versuch ist strafbar. (3) In besonders schweren Fällen ist die Strafe Freiheitsstrafe von einem Jahr bis zu fünf Jahren. …

(4) Handelt der Täter in den Fällen des Absatzes 1 fahrlässig, so ist die Strafe Freiheitsstrafe bis zu einem Jahr oder Geldstrafe

§ 41 Strafvorschriften

Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bei Inverkehrbringen oder Inbetriebnahme

1. entgegen § 4 Abs. 2 Satz 1 in Verbindung mit Satz 2
2. entgegen § 6 Abs. 1 Satz 1 ein Medizinprodukt, das nicht den Vorschriften der Strahlenschutzverordnung oder der Röntgenverordnung unterliegt oder bei dessen Herstellung ionisierende Strahlen nicht verwendet wurden
3. … ein Medizinprodukt, mit der CE-Kennzeichnung versieht,
4. … mit einer klinischen Prüfung beginnt, eine klinische Prüfung durchführt oder eine klinische Prüfung fortsetzt,
5. … mit einer Leistungsbewertungsprüfung beginnt, eine Leistungsbewertungsprüfung durchführt/fortsetzt

§ 42 Bußgeldvorschriften

(3) … Ordnungswidrigkeit … Geldbuße bis zu dreißigtausend Euro

MPBetreibV

Verordnung über das Errichten, Betreiben und Anwenden von Medizinprodukten (Medizinprodukte-Betreiberverordnung - MPBetreibV)

§ 1 Anwendungsbereich

(1) Diese Verordnung gilt für das Betreiben und Anwenden von Medizinprodukten im Sinne des Medizinproduktegesetzes einschließlich der damit zusammenhängenden Tätigkeiten.

(2) Diese Verordnung gilt nicht für Medizinprodukte 1. zur klinischen Prüfung, 2. zur Leistungsbewertungsprüfung oder 3. die in ausschließlich eigener Verantwortung für persönliche Zwecke erworben und angewendet werden.

(3) Die Vorschriften des Arbeitsschutzgesetzes sowie die Rechtsvorschriften, die aufgrund des Arbeitsschutzgesetzes erlassen wurden, sowie Unfallverhütungsvorschriften bleiben unberührt.

MPBetreibV

§ 3 Pflichten eines Betreibers

(1) Der Betreiber hat die ihm nach dieser Verordnung obliegenden Pflichten wahrzunehmen, um ein sicheres und ordnungsgemäßes Anwenden der in seiner Gesundheitseinrichtung am Patienten eingesetzten Medizinprodukte zu gewährleisten.

(2) Die Pflichten eines Betreibers hat auch wahrzunehmen, wer Patienten mit Medizinprodukten zur Anwendung durch sich selbst oder durch Dritte in der häuslichen Umgebung oder im sonstigen privaten Umfeld aufgrund einer gesetzlichen oder vertraglichen Verpflichtung versorgt. …

MPBetreibV

§ 4 Allgemeine Anforderungen

(1) Medizinprodukte dürfen nur ihrer Zweckbestimmung … Regeln der Technik betrieben und angewendet werden.

(2) Medizinprodukte .. nur von Personen betrieben … werden, die die dafür erforderliche Ausbildung oder Kenntnis und Erfahrung besitzen.

(3) Eine Einweisung in die ordnungsgemäße Handhabung des Medizinproduktes ist erforderlich. … Die Einweisung …ist in geeigneter Form zu dokumentieren.

(4) … verbundene Medizinprodukte sowie mit Zubehör einschließlich Software oder mit anderen Gegenständen verbundene Medizinprodukte dürfen … betrieben … werden, wenn sie … geeignet sind.

(5) Der Betreiber darf nur Personen mit dem Anwenden von Medizinprodukten beauftragen, die … eingewiesen sind.

MPBetreibV

§ 4 Allgemeine Anforderungen

(6) Der Anwender hat sich vor dem Anwenden eines Medizinproduktes von der Funktionsfähigkeit und dem ordnungsgemäßen Zustand des Medizinproduktes zu überzeugen und die Gebrauchsanweisung … zu beachten. …

(7) Die Gebrauchsanweisung und die dem Medizinprodukt beigefügten Hinweise sind so aufzubewahren, dass die … Angaben dem Anwender jederzeit zugänglich sind.

§ 5 Besondere Anforderungen

Sofern für eine Tätigkeit nach dieser Verordnung besondere Anforderungen vorausgesetzt werden, darf diese Tätigkeit nur durchführen, wer

1. hinsichtlich der jeweiligen Tätigkeit über aktuelle Kenntnisse aufgrund einer geeigneten Ausbildung und einer einschlägigen beruflichen Tätigkeit verfügt,
2. hinsichtlich der fachlichen Beurteilung keiner Weisung unterliegt und
3. über die Mittel, insbesondere Räume, Geräte und sonstige Arbeitsmittel, wie geeignete Mess- und Prüfeinrichtungen, verfügt, die erforderlich sind, die jeweilige Tätigkeit ordnungsgemäß und nachvollziehbar durchzuführen.

MPBetreibV

§ 6 Beauftragter für Medizinproduktesicherheit

(1) Gesundheitseinrichtungen mit regelmäßig mehr als 20 Beschäftigten … Beauftragter für Medizinproduktesicherheit bestimmt ist.

(2) Der Beauftragte für Medizinproduktesicherheit nimmt … folgende Aufgaben für den Betreiber wahr: 1. die Aufgaben einer Kontaktperson … mit Meldungen über Risiken von Medizinprodukten … Umsetzung von … korrektiven Maßnahmen, 2. die Koordinierung interner Prozesse der Gesundheitseinrichtung zur Erfüllung der Melde- und Mitwirkungspflichten …

3. Koordinierung / Umsetzung Maßnahmen und Rückrufmaßnahmen …

(4) Die Gesundheitseinrichtung hat sicherzustellen, dass eine FunktionsE-Mail-Adresse des Beauftragten für die Medizinproduktesicherheit auf ihrer Internetseite bekannt gemacht ist.

MPBetreibV

§ 9 Qualitätssicherungssystem für medizinische Laboratorien

(1) Wer laboratoriumsmedizinische Untersuchungen durchführt, hat vor Aufnahme dieser Tätigkeit ein Qualitätssicherungssystem … einzurichten. …

(2) Die Unterlagen über das eingerichtete Qualitätssicherungssystem sind für die Dauer von fünf Jahren aufzubewahren, sofern aufgrund anderer Vorschriften keine längere Aufbewahrungsfrist vorgeschrieben ist.

MPBetreibV

§ 11 Sicherheitstechnische Kontrollen

(1)Der Betreiber hat für die … Medizinprodukte sicherheitstechnische Kontrollen nach den allgemein anerkannten Regeln der Technik … durchzuführen oder durchführen zu lassen. Er hat … Fristen vorzusehen, dass … Mängel, … rechtzeitig festgestellt werden können. … spätestens alle zwei Jahre mit Ablauf des Monats durchzuführen, in dem die Inbetriebnahme des Medizinproduktes erfolgte oder die letzte sicherheitstechnische Kontrolle durchgeführt wurde. …

(3) Über die sicherheitstechnische Kontrolle ist ein Protokoll anzufertigen, … Das Protokoll … hat der Betreiber zumindest bis zur nächsten sicherheitstechnischen Kontrolle aufzubewahren.

(4) Der Betreiber darf mit der Durchführung der sicherheitstechnischen Kontrollen nur Personen, Betriebe oder Einrichtungen beauftragen, die … die Voraussetzungen … des jeweiligen Medizinproduktes erfüllen.

MPBetreibV

§ 12 Medizinproduktebuch

(1) Für die in den Anlagen 1 und 2 aufgeführten Medizinprodukte hat der Betreiber ein Medizinproduktebuch nach Absatz 2 zu führen. …

(3) Das Medizinproduktebuch ist so aufzubewahren, dass die Angaben dem Anwender während der Arbeitszeit zugänglich sind. Nach der Außerbetriebnahme des Medizinproduktes ist das Medizinproduktebuch noch fünf Jahre aufzubewahren.

§ 13 Bestandsverzeichnis

(1) Der Betreiber hat für alle aktiven nichtimplantierbaren Medizinprodukte der jeweiligen Betriebsstätte ein Bestandsverzeichnis zu führen. …

MPBetreibV

§ 17 Ordnungswidrigkeiten (Auszüge)

Ordnungswidrig im Sinne des § 42 Absatz 2 Nummer 16 des Medizinproduktegesetzes handelt, wer vorsätzlich oder fahrlässig

1… ein dort genanntes Medizinprodukt betreibt oder anwendet,

2. … nicht sicherstellt, dass ein Beauftragter für Medizinproduktesicherheit bestimmt ist,

3. … nicht sicherstellt, dass eine Funktions-E-Mail-Adresse bekannt gemacht ist,

4. … eine Person, einen Betrieb oder eine Einrichtung beauftragt (die/der nicht geeignet ist)

7. Qualitätssicherungssystem nicht, nicht richtig, … einrichtet,

8. … eine Kontrolle nicht, … durchführen lässt,

9. … ein dort genanntes Protokoll nicht oder nicht für die vorgeschriebene Dauer aufbewahrt,

15. … Aufzeichnung nicht, … oder nicht mindestens 20 Jahre

Neuer europäischer Rechtsrahmen für Medizinprodukte ab 2017

Am 5. Mai 2017 wurde im *Amtsblatt der Europäischen Union die Verordnung (EU) 2017/745 vom 5. April 2017 über Medizinprodukte (MDR)* veröffentlicht, die die bisherigen Richtlinien und Verordnungen ändert bzw. aufhebt.

Es entfällt die Umsetzung in nationales Recht der einzelnen Mitgliedsstaaten, sie ist seit 25. Mai 2017 in Kraft. Sie gilt in weiten Teilen ab dem 26. Mai 2020. Innerhalb der bis dahin geltenden Übergangsfrist können sich Hersteller wahlweise noch nach altem Recht (Richtlinien 90/385/EWG und 93/42/EWG) oder bereits nach neuem Recht (MDR) zertifizieren lassen. Benannte Stellen können sich seit 11/2017 neu benennen lassen. Mit dem Eintritt des „Geltungsbeginns“ (drei Jahre nach dem Datum des Inkrafttretens) endet die Wahlmöglichkeit der Hersteller. Altzertifikate behalten bis zu vier Jahren ihre Gültigkeit.

Artikel 1

Gegenstand und Geltungsbereich

(1) Mit dieser Verordnung werden Regeln für das Inverkehrbringen, die Bereitstellung auf dem Markt und die Inbetriebnahme von für den menschlichen Gebrauch bestimmten Medizinprodukten und deren Zubehör in der Union festgelegt. Diese Verordnung gilt ferner für in der Union durchgeführte klinische Prüfungen, die diese Medizinprodukte und dieses Zubehör betreffen.

(2) ….

Diese Verordnung gilt zudem für in der Union durchgeführte klinische Prüfungen, die die in Unterabsatz 1 genannten Produkte betreffen.

MDR

Artikel 17

Einmalprodukte und ihre Aufbereitung

(1) Die Aufbereitung und Weiterverwendung von Einmalprodukten ist nur gemäß diesem Artikel und nur dann zulässig, wenn sie nach nationalem Recht gestattet ist.

Artikel 19

EU-Konformitätserklärung

Artikel 20

CE-Konformitätskennzeichnung

Artikel 63

Einwilligung nach Aufklärung

(1) Die Einwilligung nach Aufklärung wird nach entsprechender Aufklärung … vom Prüfungsteilnehmer … schriftlich erteilt, datiert und unterzeichnet. …

(weitere Artikel 64/65/66)

Artikel 69

Schadensersatz

(1) Die Mitgliedstaaten stellen sicher, dass Verfahren zur Entschädigung für jeden Schaden, der einem Prüfungsteilnehmer durch seine Teilnahme an einer klinischen Prüfung auf ihrem Hoheitsgebiet entsteht, in Form einer Versicherung oder einer Garantie oder ähnlichen Regelungen bestehen, die hinsichtlich ihres Zwecks gleichartig sind und der Art und dem Umfang des Risikos entsprechen.

(2) Der Sponsor und der Prüfer wenden das Verfahren gemäß Absatz 1 in einer Weise an, die dem Mitgliedstaat, in dem die klinische Prüfung durchgeführt wird, entspricht.

Artikel 87

Meldung von schwerwiegenden Vorkommnissen und Sicherheitskorrekturmaßnahmen im Feld

(1) Hersteller von Produkten, die auf dem Unionsmarkt bereitgestellt werden, ausgenommen Prüfprodukte, melden … Folgendes: a) Jedes schwerwiegende Vorkommnis … b) jede Sicherheitskorrekturmaßnahme ...

(3) Die Hersteller melden jedes schwerwiegende Vorkommnis … unverzüglich, nachdem sie einen Kausalzusammenhang … zwischen dem Vorkommnis und ihrem Produkt festgestellt haben, spätestens jedoch 15 Tage, nachdem sie Kenntnis … erhalten haben.

(4) … im Falle einer schwerwiegenden Gefahr für die öffentliche Gesundheit … Meldung … unverzüglich, spätestens jedoch zwei Tage, nachdem der Hersteller Kenntnis von dieser Gefahr erhalten hat.

(5) im Falle des Todes … unverzüglich …

Artikel 95

Verfahren für den Umgang mit Produkten, die ein unvertretbares Gesundheits- und Sicherheitsrisiko darstellen

(3) Die Wirtschaftsakteure gemäß Absatz 1 sorgen unverzüglich dafür, dass alle geeigneten Korrekturmaßnahmen in der gesamten Union in Bezug auf sämtliche betroffenen Produkte, die sie auf dem Markt bereitgestellt haben, ergriffen werden.

KAPITEL IX

VERTRAULICHKEIT, DATENSCHUTZ, FINANZIERUNG UND SANKTIONEN

Artikel 109

Vertraulichkeit

(1) Sofern in dieser Verordnung nichts anderes vorgesehen ist, wahren alle an der Anwendung dieser Verordnung beteiligten Parteien … die Vertraulichkeit der im Rahmen der Durchführung ihrer Tätigkeiten erlangten Informationen und Daten, um Folgendes zu gewährleisten:

a) den Schutz personenbezogener Daten gemäß Artikel 110;

b) den Schutz vertraulicher Geschäftsdaten und der Betriebs- und Geschäftsgeheimnisse einer natürlichen oder juristischen Person, einschließlich der Rechte des geistigen Eigentums, …

c) die wirksame Durchführung dieser Verordnung, insbesondere in Bezug auf Kontrollen, Untersuchungen und Audits.

KAPITEL IX

VERTRAULICHKEIT, DATENSCHUTZ, FINANZIERUNG UND SANKTIONEN

Artikel 110

Datenschutz

(1) Bei der Verarbeitung personenbezogener Daten im Rahmen der Durchführung dieser Verordnung beachten die Mitgliedstaaten die Richtlinie 95/46/EG. (abgelöst durch die EU-DSGVO)

Artikel 123

Inkrafttreten und Geltungsbeginn

(1) Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft.

(2) Sie gilt ab dem 26. Mai 2020.

(3) Abweichend von Absatz 2 gilt Folgendes: a) Die Artikel 35 bis 50 gelten ab dem 26. November 2017. Die den Benannten Stellen gemäß den Artikeln 35 bis 50 erwachsenden Verpflichtungen gelten jedoch von dem genannten Tag an bis zum 26. Mai 2020 nur für diejenigen Stellen, die einen Antrag auf Benennung gemäß Artikel 38 einreichen;

b) die Artikel 101 und 103 gelten ab dem 26. November 2017;

c) Artikel 102 gilt ab dem 26. Mai 2018;

Verordnung über den Schutz vor Schäden durch Röntgenstrahlen (Röntgenverordnung - RöV)

§ 1 Anwendungsbereich

Diese Verordnung gilt für Röntgeneinrichtungen und Störstrahler, in denen Röntgenstrahlung mit einer Grenzenergie von mindestens fünf Kiloelektronvolt durch beschleunigte Elektronen erzeugt werden kann und bei denen die Beschleunigung der Elektronen auf eine Energie von einem Megaelektronvolt begrenzt ist.

§ 3 Genehmigungsbedürftiger Betrieb von Röntgeneinrichtungen

(1) Wer eine Röntgeneinrichtung betreibt oder deren Betrieb wesentlich verändert, bedarf der Genehmigung.

(3) Für eine Genehmigung zum Betrieb einer Röntgeneinrichtung zur Anwendung von Röntgenstrahlung am Menschen müssen zusätzlich zu Absatz 2 folgende Voraussetzungen erfüllt sein:

1. Der Antragsteller oder der von ihm bestellte Strahlenschutzbeauftragte ist als Arzt oder Zahnarzt approbiert oder ihm ist die vorübergehende Ausübung des ärztlichen oder zahnärztlichen Berufs erlaubt; …

§ 13 Strahlenschutzverantwortliche und Strahlenschutzbeauftragte

(1) Strahlenschutzverantwortlicher ist, wer einer Genehmigung nach § 3 oder § 5 bedarf oder wer eine Anzeige nach § 4 zu erstatten hat. Handelt es sich bei dem Strahlenschutzverantwortlichen um eine juristische Person oder um eine rechtsfähige Personengesellschaft, werden die Aufgaben des Strahlenschutzverantwortlichen von der durch Gesetz, Satzung oder Vertrag zur Vertretung berechtigten Person wahrgenommen. …

(2) Soweit dies für den sicheren Betrieb notwendig ist, hat der Strahlenschutzverantwortliche für die Leitung oder Beaufsichtigung dieses Betriebes die erforderliche Anzahl von Strahlenschutzbeauftragten schriftlich zu bestellen.

§ 15 Pflichten des Strahlenschutzverantwortlichen und des Strahlenschutzbeauftragten

(1) Der Strahlenschutzverantwortliche hat unter Beachtung des Standes der Technik zum Schutz des Menschen und der Umwelt vor den schädlichen Wirkungen von Röntgenstrahlung durch geeignete Schutzmaßnahmen, insbesondere durch Bereitstellung geeigneter Räume, Schutzvorrichtungen, Geräte und Schutzausrüstungen für Personen, durch geeignete Regelung des Betriebsablaufs und durch Bereitstellung ausreichenden und geeigneten Personals, erforderlichenfalls durch Außerbetriebsetzung, dafür zu sorgen, dass
1. jede unnötige Strahlenexposition von Menschen vermieden wird,

…

§ 18 Sonstige Pflichten beim Betrieb einer Röntgeneinrichtung oder eines Störstrahlers nach § 5 Abs. 1

(1) Es ist dafür zu sorgen, dass

1. … Personen anhand einer deutschsprachigen Gebrauchsanweisung durch eine entsprechend qualifizierte Person in die sachgerechte Handhabung eingewiesen werden und über die Einweisung unverzüglich Aufzeichnungen angefertigt werden,

2. eine Ausfertigung des Genehmigungsbescheides … aufbewahrt wird,

3. die Gebrauchsanweisung nach Nummer 1 und die Bescheinigung nach § 4 Abs. 2 Nr. 1, der letzte Prüfbericht … bereitgehalten werden, 4. … Text dieser Verordnung zur Einsicht … verfügbar gehalten wird, 5. eine Röntgeneinrichtung in Zeitabständen von längstens fünf Jahren … überprüft und eine Durchschrift des … Prüfberichts den zuständigen Stellen unverzüglich übersandt wird und

6. bei einer Röntgeneinrichtung zur Anwendung von Röntgenstrahlung am Menschen ein aktuelles Bestandsverzeichnis geführt … wird; …

§ 24 Berechtigte Personen

(1) In der Heilkunde oder Zahnheilkunde darf Röntgenstrahlung am Menschen nur angewendet werden von

1. Personen, die als Ärzte approbiert sind … und die für das Gesamtgebiet der Röntgenuntersuchung oder Röntgenbehandlung die erforderliche Fachkunde im Strahlenschutz besitzen,

2. Personen, die als Ärzte oder Zahnärzte approbiert sind oder denen die Ausübung des ärztlichen oder zahnärztlichen Berufs erlaubt ist und die für das Teilgebiet der Anwendung von Röntgenstrahlung, in dem sie tätig sind, die erforderliche Fachkunde im Strahlenschutz besitzen,

3. Personen, die als Ärzte oder Zahnärzte approbiert sind oder zur Ausübung des ärztlichen oder zahnärztlichen Berufs berechtigt sind und nicht über die erforderliche Fachkunde im Strahlenschutz verfügen, wenn sie unter ständiger Aufsicht und Verantwortung einer Person nach Nummer 1 oder 2 tätig sind und über die erforderlichen Kenntnisse im Strahlenschutz verfügen.

§ 28 Aufzeichnungspflichten, Röntgenpass

(1) Es ist dafür zu sorgen, dass über jede Anwendung von Röntgenstrahlung am Menschen Aufzeichnungen nach Maßgabe des Satzes 2 angefertigt werden. Die Aufzeichnungen müssen enthalten: …

Die Aufzeichnungen sind gegen unbefugten Zugriff und unbefugte Änderung zu sichern. Sie sind auf Verlangen der zuständigen Behörde vorzulegen; dies gilt nicht für die medizinischen Befunde.

(3) Aufzeichnungen über Röntgenbehandlungen sind 30 Jahre lang nach der letzten Behandlung aufzubewahren. Röntgenbilder und die Aufzeichnungen … sind zehn Jahre lang nach der letzten Untersuchung aufzubewahren. Röntgenbilder und die Aufzeichnungen von Röntgenuntersuchungen einer Person, die das 18. Lebensjahr noch nicht vollendet hat, sind bis zur Vollendung des 28. Lebensjahres dieser Person aufzubewahren.

§ 28 Aufzeichnungspflichten, Röntgenpass

(4) Röntgenbilder und die Aufzeichnungen nach Absatz 1 Satz 2 können als Wiedergabe auf einem Bildträger oder auf anderen Datenträgern aufbewahrt werden, wenn sichergestellt ist, dass …

1. mit den Bildern oder Aufzeichnungen bildlich oder inhaltlich übereinstimmen, wenn sie lesbar gemacht werden und

2. während der Dauer der Aufbewahrungsfrist verfügbar sind und jederzeit innerhalb angemessener Zeit lesbar gemacht werden können, und sichergestellt ist, dass während der Aufbewahrungszeit keine Informationsänderungen oder –Verluste eintreten können. …

3. nachträgliche Änderungen / Ergänzungen als solche erkennbar sind …

4. während der Dauer der Aufbewahrung die Verknüpfung der personenbezogenen Patientendaten mit dem erhobenen Befund, … jederzeit hergestellt werden kann.

§ 42 Meldepflicht

(1) Außergewöhnliche Ereignisabläufe oder Betriebszustände beim Betrieb einer Röntgeneinrichtung oder eines Störstrahlers nach § 5 Abs.

1 sind der zuständigen Behörde unverzüglich zu melden, wenn 1. zu besorgen ist, dass eine Person eine Strahlenexposition erhalten haben kann, die die Grenzwerte der Körperdosis nach § 31a Abs. 1 oder 2 übersteigt oder

2. sie von erheblicher sicherheitstechnischer Bedeutung sind.

(2) Nach Absatz 1 meldepflichtige außergewöhnliche Ereignisabläufe oder Betriebszustände beim Betrieb einer Röntgeneinrichtung, die ein Medizinprodukt oder Zubehör im Sinne des Medizinproduktegesetzes ist, sind zusätzlich unverzüglich dem Bundesinstitut für Arzneimittel und Medizinprodukte zu melden.

§ 43 Elektronische Kommunikation

(1) Aufzeichnungs-, Buchführungs- und Aufbewahrungspflichten nach dieser Verordnung können elektronisch erfüllt werden. § 28 Absatz 4 bis 6 bleibt unberührt.

(2) Mitteilungs-, Melde- oder Anzeigepflichten können in elektronischer Form erfüllt werden, wenn der Empfänger hierfür einen Zugang eröffnet und das Verfahren und die für die Datenübertragung notwendigen Anforderungen bestimmt. Dabei müssen dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit getroffen werden, die insbesondere die Vertraulichkeit und Unversehrtheit der Daten gewährleisten; bei der Nutzung allgemein zugänglicher Netze sind Verschlüsselungsverfahren anzuwenden. Ist ein übermitteltes elektronisches Dokument für den Empfänger nicht zur Bearbeitung geeignet, teilt er dies dem Absender unter Angabe der für den Empfang geltenden technischen Rahmenbedingungen unverzüglich mit.

§ 44 Ordnungswidrigkeiten

Ordnungswidrig im Sinne des § 46 Abs. 1 Nr. 4 des Atomgesetzes handelt, wer vorsätzlich oder fahrlässig 1. ohne Genehmigung nach a) § 3 Abs.

1 eine Röntgeneinrichtung betreibt oder deren Betrieb verändert

5. entgegen § 9 Satz 1 Nr. 1 oder 2 eine Qualitätskontrolle nicht oder nicht rechtzeitig durchführt oder nicht überwachen lässt

10. entgegen § 13 Abs. 2 Satz 1 die erforderliche Anzahl von Strahlenschutzbeauftragten nicht oder nicht in der vorgeschriebenen Weise bestellt.

12. entgegen … als Strahlenschutzverantwortlicher oder Strahlenschutzbeauftragter nicht dafür sorgt, dass eine der Vorschriften der … oder § 42 eingehalten wird,

Gesetz über Ordnungswidrigkeiten (OWiG)

§ 1 Begriffsbestimmung

(1) Eine Ordnungswidrigkeit ist eine rechtswidrige und vorwerfbare Handlung, die den Tatbestand eines Gesetzes verwirklicht, das die Ahndung mit einer Geldbuße zuläßt.

(2) Eine mit Geldbuße bedrohte Handlung ist eine rechtswidrige Handlung, die den Tatbestand eines Gesetzes im Sinne des Absatzes 1 verwirklicht, auch wenn sie nicht vorwerfbar begangen ist

§ 2 Sachliche Geltung

Dieses Gesetz gilt für Ordnungswidrigkeiten nach Bundesrecht und nach Landesrecht

§ 8 Begehen durch Unterlassen

§ 9 Handeln für einen anderen

§ 10 Vorsatz und Fahrlässigkeit

Gesetz über Ordnungswidrigkeiten (OWiG)

§ 17 Höhe der Geldbuße

(1) Die Geldbuße beträgt mindestens fünf Euro und, wenn das Gesetz nichts anderes bestimmt, höchstens eintausend Euro.

(3) Grundlage für die Zumessung der Geldbuße sind die Bedeutung der Ordnungswidrigkeit und der Vorwurf, der den Täter trifft. …

(4) Die Geldbuße soll den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat, übersteigen. Reicht das gesetzliche Höchstmaß hierzu nicht aus, so kann es überschritten werden.

§ 19 Tateinheit

(2) Sind mehrere Gesetze verletzt, so wird die Geldbuße nach dem Gesetz bestimmt, das die höchste Geldbuße androht. …

§ 20 Tatmehrheit

Sind mehrere Geldbußen verwirkt, so wird jede gesondert festgesetzt.

Gesetz über Ordnungswidrigkeiten (OWiG)

§ 30 Geldbuße gegen juristische Personen und Personenvereinigungen

(1) Hat jemand

1. als vertretungsberechtigtes Organ einer juristischen Person oder als Mitglied eines solchen Organs, … eine Straftat oder Ordnungswidrigkeit begangen, durch die Pflichten, welche die juristische Person oder die Personenvereinigung treffen, verletzt worden sind oder die juristische Person oder die Personenvereinigung bereichert worden ist oder werden sollte, so kann gegen diese eine Geldbuße festgesetzt werden.

(2) Die Geldbuße beträgt

1. im Falle einer vorsätzlichen Straftat bis zu zehn Millionen Euro,
2. im Falle einer fahrlässigen Straftat bis zu fünf Millionen Euro.

G-BA

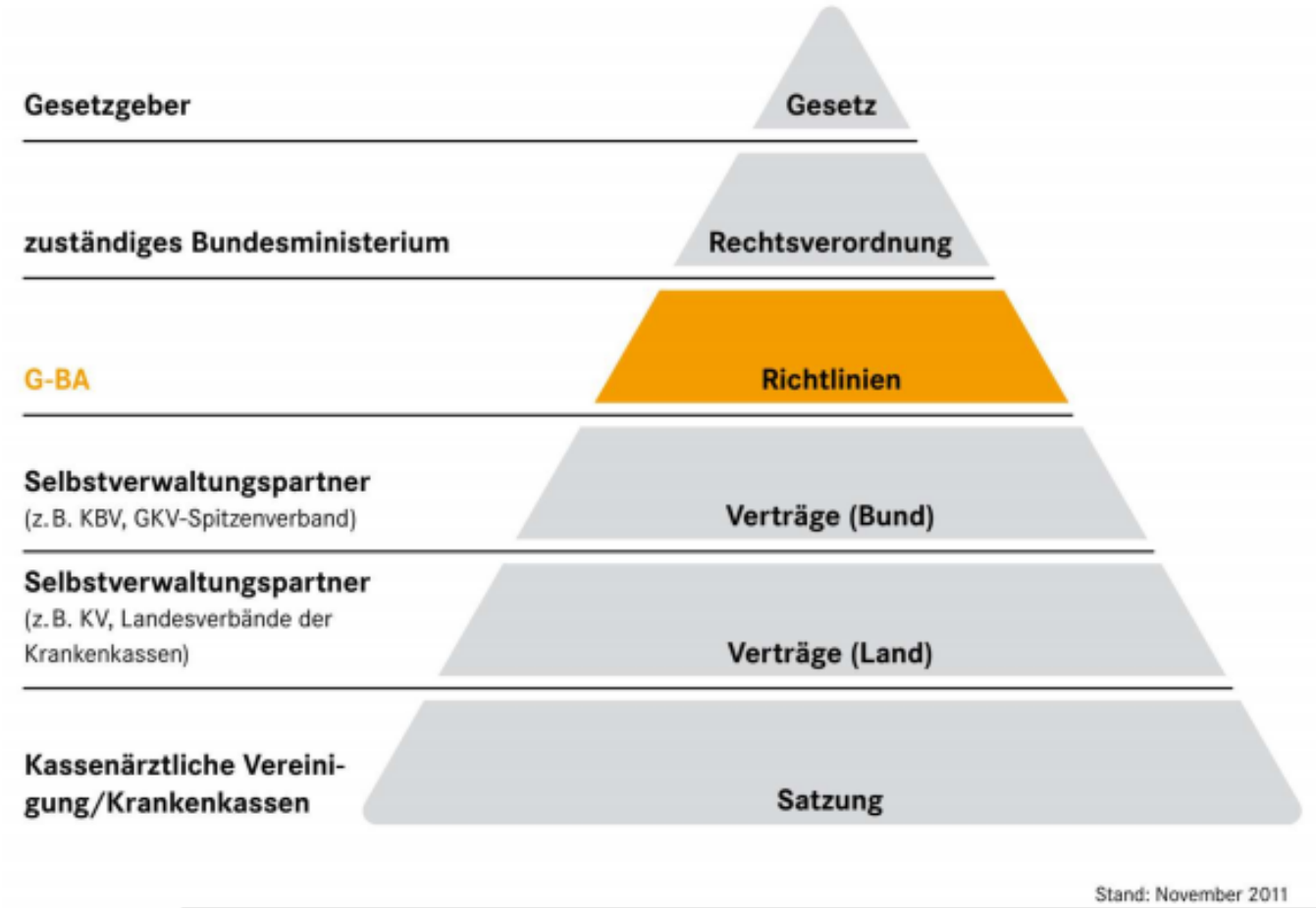
Der Gemeinsame Bundesausschuss (G-BA) ist eine juristische Person des öffentlichen Rechts und wird von den vier großen Spitzenorganisationen der Selbstverwaltung im deutschen Gesundheitswesen gebildet:

- ✓ der Kassenärztlichen und
- ✓ Kassenzahnärztlichen Bundesvereinigung,
- ✓ der Deutschen Krankenhausgesellschaft und dem
- ✓ GKV-Spitzenverband.

Neben diesen vier Trägerorganisationen sind Patientenvertreterinnen und Patientenvertreter antrags- jedoch nicht stimmberechtigt an allen Beratungen beteiligt.

Rechtsgrundlage der Arbeit des G-BA ist das Fünfte Sozialgesetzbuch (SGB V).

Die Rechtsstellung des G-BA



G-BA Richtlinien I

- ✓ Bestimmung des Gemeinsamen Bundesausschusses von Anforderungen an einrichtungsübergreifende Fehlermeldesysteme (üFMS-B)
- ✓ Regelungen des Gemeinsamen Bundesausschusses gemäß § 136b Absatz 1 Satz 1 Nummer 3 SGB V über Inhalt, Umfang und Datenformat eines strukturierten Qualitätsberichts für nach § 108 SGB V zugelassene Krankenhäuser (Regelungen zum Qualitätsbericht der Krankenhäuser, Qb-R)

G-BA Richtlinien II

- ✓ Richtlinie des Gemeinsamen Bundesausschusses nach § 92 Abs. 1 Satz 2 Nr. 13 i. V. m. § 136 Abs. 1 Nr. 1 SGB V über die einrichtungs- und sektorenübergreifenden Maßnahmen der Qualitätssicherung (Richtlinie zur einrichtungs- und sektorenübergreifenden Qualitätssicherung – Qesü-RL)
- ✓ Richtlinie des Gemeinsamen Bundesausschusses über grundsätzliche Anforderungen an ein einrichtungsinternes Qualitätsmanagement für Vertragsärztinnen und Vertragsärzte, Vertragspsychotherapeutinnen und Vertragspsychotherapeuten, medizinische Versorgungszentren, Vertragszahnärztinnen und Vertragszahnärzte sowie zugelassene Krankenhäuser (Qualitätsmanagement-Richtlinie/QM-RL)

G-BA Richtlinien III

- ✓ Richtlinie des Gemeinsamen Bundesausschusses gemäß § 136 Abs. 1 SGB V i. V. m. § 135a SGB V über Maßnahmen der Qualitätssicherung für nach § 108 SGB V zugelassene Krankenhäuser (Richtlinie über Maßnahmen der Qualitätssicherung in Krankenhäusern / QSKH-RL)
- ✓ Richtlinie des Gemeinsamen Bundesausschusses zu Auswahl, Umfang und Verfahren bei Qualitätsprüfungen im Einzelfall nach § 136 Abs. 2 SGB V („Qualitätsprüfungs-Richtlinie vertragsärztliche Versorgung“)

G-BA üFMS-B

Bestimmung des Gemeinsamen Bundesausschusses von Anforderungen an einrichtungsübergreifende Fehlermeldesysteme (üFMS-B)

§ 1 Anwendungsbereich

(1) 1Zur Erfüllung des in § 136a Absatz 3 Satz 3 SGB V geregelten Auftrags bestimmt der Gemeinsame Bundesausschuss (G-BA) nachfolgend die Anforderungen an einrichtungsübergreifende Fehlermeldesysteme (üFMS), die in besonderem Maße geeignet erscheinen, Risiken und Fehlerquellen in der stationären Versorgung zu erkennen, auszuwerten und zur Vermeidung unerwünschter Ereignisse beizutragen. Diese Anforderungen bilden die Grundlage für die Vereinbarung von Zuschlägen im Sinne von § 17b Absatz 1a Nummer 4 des Krankenhausfinanzierungsgesetzes (KHG).

G-BA üFMS-B

§ 2 Definitionen

(1) Ein üFMS im Sinne dieser Bestimmung ist eine Berichts- und Lernplattform für sicherheitsrelevante Ereignisse und Risiken im Gesundheitswesen, an dem mehrere Einrichtungen teilnehmen.

(2) Eine Einrichtung im Sinne dieser Bestimmung ist ein nach § 108 SGB V zugelassenes Krankenhaus oder … ein einzelner Krankenhausstandort mit einer Verpflichtung zu einem standortspezifischen Qualitätsbericht gemäß den Regelungen zum Qualitätsbericht der Krankenhäuser (Qb-R).

(3) Die Teilnahme an einem üFMS im Sinne dieser Bestimmung liegt vor, wenn die Einrichtung sowohl durch die aktive Meldung als auch durch die Nutzung der in der Falldatenbank des üFMS enthaltenen Fallbeschreibungen und Kommentare teilnimmt.

G-BA üFMS-B

§ 3 Anforderungen an ein einrichtungsübergreifendes Fehlermeldesystem

(1) Die Erfüllung der nachfolgenden Anforderungen an ein üFMS ist Grundlage für die Vereinbarung von Zuschlägen im Sinne von § 17b Absatz 1a Nummer 4 KHG:

1. Das üFMS ist für alle Einrichtungen offen und über das Internet frei zugänglich.

2. Ein üFMS nimmt Meldungen zu kritischen und unerwünschten Ereignissen sowie Fehlern, Beinahe-Schäden und sonstigen Risiken möglichst mit schon abgeleiteten Empfehlungen zu deren Vermeidung entgegen. Nicht zulässig ist die Übermittlung und Verarbeitung personenbezogener Daten von Patientinnen und Patienten. Es ist eine vertrauliche Bearbeitung aller Daten sowie eine sichere Übertragung und Speicherung der Daten zu gewährleisten. Jegliche Möglichkeit zur Rückverfolgung der meldenden Einrichtungen von veröffentlichten Fällen ist auszuschließen.

G-BA üFMS-B

§ 3 Anforderungen an ein einrichtungsübergreifendes Fehlermeldesystem

3. Zur Eingabe von Meldungen existiert ein strukturiertes Meldeformular. Für einen reibungslosen Datenaustausch zwischen den einrichtungsinternen Fehlermeldesystemen der meldenden Einrichtungen und dem üFMS bestehen Schnittstellen (Import-, Exportfunktion). Eingehende Meldungen werden themenbezogen kategorisiert und nach Relevanz klassifiziert.

(2) Auf Anforderung der teilnehmenden Einrichtung hat der verantwortliche Betreiber des üFMS einen entsprechenden Nachweis über die getroffenen Vorkehrungen zur Erfüllung der Anforderungen gemäß Absatz 1 zu führen.

G-BA Qb-R

Regelungen des Gemeinsamen Bundesausschusses gemäß § 136b Absatz 1 Satz 1 Nummer 3 SGB V über Inhalt, Umfang und Datenformat eines strukturierten Qualitätsberichts für nach § 108 SGB V zugelassene Krankenhäuser (Regelungen zum Qualitätsbericht der Krankenhäuser, Qb-R)

§ 1 Ziele des Qualitätsberichts Die Ziele des Qualitätsberichts umfassen:

- ✓ Verbesserung von Transparenz und Qualität der Versorgung im Kh
- ✓ Information, Orientierungs- und Entscheidungshilfe für alle int. Pers.
- ✓ Schaffung einer Grundlage für vergleichende Informationen … über die Qualität der Versorgung im Krankenhaus,
- ✓ Möglichkeit für ein Krankenhaus, Leistungen transparent und sichtbar darzustellen.

G-BA Qb-R

§ 4 Datenformat des Qualitätsberichts

Der Qualitätsbericht ist nach Maßgabe der Anlage 1 für das jeweilige Berichtsjahr in maschinenverwertbarer Form zu erstellen.

§ 6 Verfahren und Fristen der Übermittlung des Qualitätsberichts

(1) Das Krankenhaus hat den Qualitätsbericht an eine Annahmestelle zu übermitteln. ...

(2) … die krankenhausbezogenen Angaben der datengestützten einrichtungsübergreifenden Qualitätssicherung … direkt von den mit der Durchführung der datengestützten einrichtungsübergreifenden Qualitätssicherung beauftragten Stellen an die Annahmestelle übermittelt. …

G-BA Qesü-RL

Richtlinie des Gemeinsamen Bundesausschusses nach § 92 Abs. 1 Satz 2 Nr. 13 i. V. m. § 136 Abs. 1 Nr. 1 SGB V über die einrichtungs- und sektorenübergreifenden Maßnahmen der Qualitätssicherung (Richtlinie zur einrichtungs- und sektorenübergreifenden Qualitätssicherung – Qesü-RL)

§1 Geltungsbereich

1. Diese Richtlinie gilt für einrichtungs- und sektorenübergreifende Verfahren.

2. Einrichtungsübergreifend sind Verfahren, die zur Beurteilung der Qualität einer Leistungserbringerin oder eines Leistungserbringers auf Vergleich mit anderen Leistungserbringerinnen und Leistungserbringern aufbauen.

G-BA Qesü-RL

§1 Geltungsbereich

(4) Diese Richtlinie gilt gemäß § 135 a Abs. 2, § 136 Abs. 1 und 2, § 299 Absatz 1 a SGB V insbesondere für:

1. nach § 108 SGB V zugelassene Krankenhäuser,

2. zur vertragsärztlichen oder vertragszahnärztlichen Versorgung zugelassene Leistungserbringerinnen und Leistungserbringer, zugelassene medizinische Versorgungszentren sowie ermächtigte Ärztinnen, Ärzte, Zahnärztinnen und Zahnärzte, Psychotherapeutinnen und Psychotherapeuten und ermächtigte ärztlich oder zahnärztlich geleitete Einrichtungen

3. Krankenkassen

G-BA Qesü-RL

§4 Beauftragungsgrundsätze

1. Der G-BA wählt das jeweilige sektorenübergreifende Thema in einem strukturierten und transparenten Verfahren auf Grundlage seiner zum jeweiligen Zeitpunkt gültigen Verfahrensordnung aus. 2. Im Auftrag des G-BA entwickelt das Institut nach § 137a SGB V die Instrumente und Qualitätsindikatoren, die notwendige Dokumentation und die EDV-technische Aufbereitung der Dokumentation, der Datenübermittlung, des abgestimmten Pseudonymisierungsverfahrens nach § 3 Absatz 2 Satz 4 der Anlage und Prozesse zum Datenfehlermanagement sowie die EDVtechnischen Vorgaben zur Datenprüfung und ein Datenprüfprogramm für das ausgewählte Thema. 2Sofern vom G-BA beauftragt, führt das Institut nach § 137a SGB V für die entwickelten Verfahren eine EDV-technische Machbarkeitsprüfung und einen Probebetrieb durch.

§13 Grundmodell des Datenflusses

1. Der Fluss der Daten erfolgt grundsätzlich elektronisch und in elektronisch auswertbarer Form unter Einbeziehung einer Datenannahmestelle und einer Vertrauensstelle an die Bundesauswertungsstelle.

2. Der G-BA legt in den themenspezifischen Bestimmungen jeweils die erforderlichen Daten fest. Er gibt die Softwarespezifikationen für die Erfassung der Daten nach § 14 vor. …

§24 Information der Patientinnen und Patienten

Die Leistungserbringerinnen und Leistungserbringer sind verpflichtet, ihre Patientinnen und Patienten etwa anhand von Merkblättern in verständlicher Weise über Zweck und Inhalt des sie betreffenden Qualitätssicherungsverfahrens zu informieren. Dies umfasst eine Information über die zu erhebenden Daten, die erhebenden und verarbeitenden Stellen sowie die Verwendung der Daten und den weiteren Umgang mit ihnen. Patientinnen und Patienten erhalten auch Hinweise auf patientenrelevante Informationsquellen unter Berücksichtigung von Empfehlungen der maßgeblichen Organisationen nach § 140f SGB V.

Teil 2: Themenspezifische Bestimmungen

Verfahren 1: Perkutane Koronarintervention (PCI) und Koronarangiographie

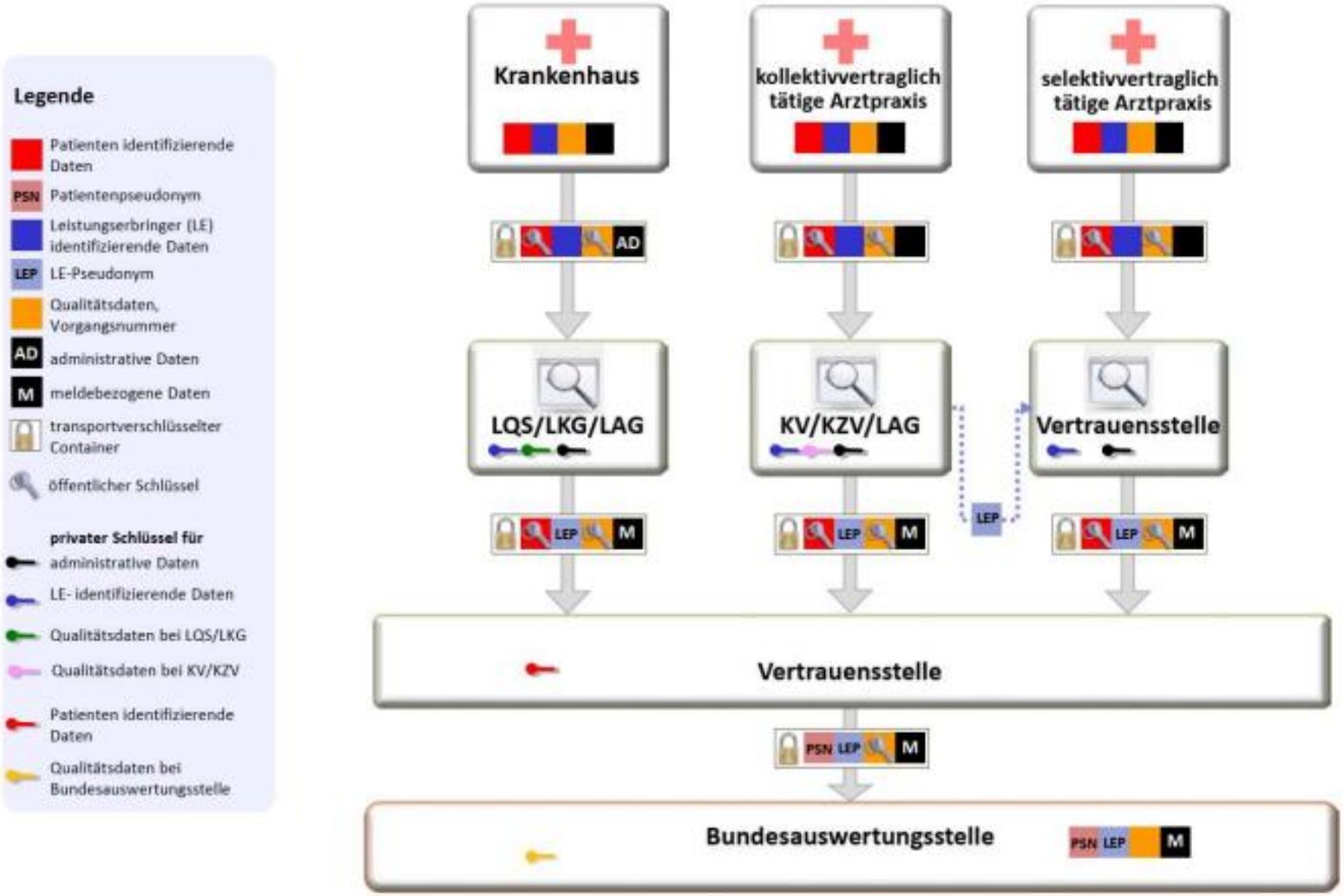
Abschnitt B:

Erhebung, Weiterleitung, Prüfung und Auswertung der Daten §5 Festlegung der zu erhebenden Daten

(2) Zum Zwecke einer bundeseinheitlichen und softwarebasierten Dokumentation durch die Leistungserbringer sowie zur Anwendung einheitlicher Regeln für die Datenbereitstellung durch die Krankenkassen erarbeitet das Institut nach § 137a SGB V, auf Grundlage der Themenspezifischen Bestimmungen und der Daten gemäß Absatz 1, Vorgaben für die anzuwendenden elektronischen Datensatzformate sowie Softwarespezifikationen. …

Ähnliches gilt für weitere Verfahren

G-BA Qesü-RL – serielles Datenflussmodell



G-BA Qesü-RL

Richtlinie des Gemeinsamen Bundesausschusses gemäß § 136 Abs. 1 SGB V i. V. m. § 135a SGB V über Maßnahmen der Qualitätssicherung für nach § 108 SGB V zugelassene Krankenhäuser (Richtlinie über Maßnahmen der Qualitätssicherung in Krankenhäusern / QSKH-RL)

§ 1 Zweck und Rechtsgrundlage der Richtlinie

(1) Zweck der Richtlinie ist insbesondere: 1. die Umsetzung der verpflichtenden Maßnahmen der Qualitätssicherung nach § 136 Abs. 1 Nr. 1 Sozialgesetzbuch (SGB) V …

G-BA Qesü-RL

B. Maßnahmen der Externen stationären Qualitätssicherung

§ 4 Einbezogene Leistungen

(1) Zur Sicherung der Qualität von Krankenhausleistungen sind nach § 108 SGB V zugelassene Krankenhäuser verpflichtet, definierte Leistungsbereiche gemäß den Anlagen 1 bis 3 zu dokumentieren. 2Dabei hat die Dokumentation bei nach § 108 SGB V zugelassenen Krankenhäusern mit einem nach Standorten differenzierten Versorgungsauftrag standortbezogen zu erfolgen. Die Darstellung der Inhalte der einbezogenen Leistungen steht als Auslöser (Ein und/oder Ausschlusskriterien sowie die dazu gehörigen Spezifikationen, die auch die EDV-technischen Vorgaben zur Datenprüfung und zur Risikostatistik enthalten) zur Verfügung und wird durch den G-BA beschlossen. Die einbezogenen Leistungen werden regelmäßig überprüft und fortgeschrieben. …

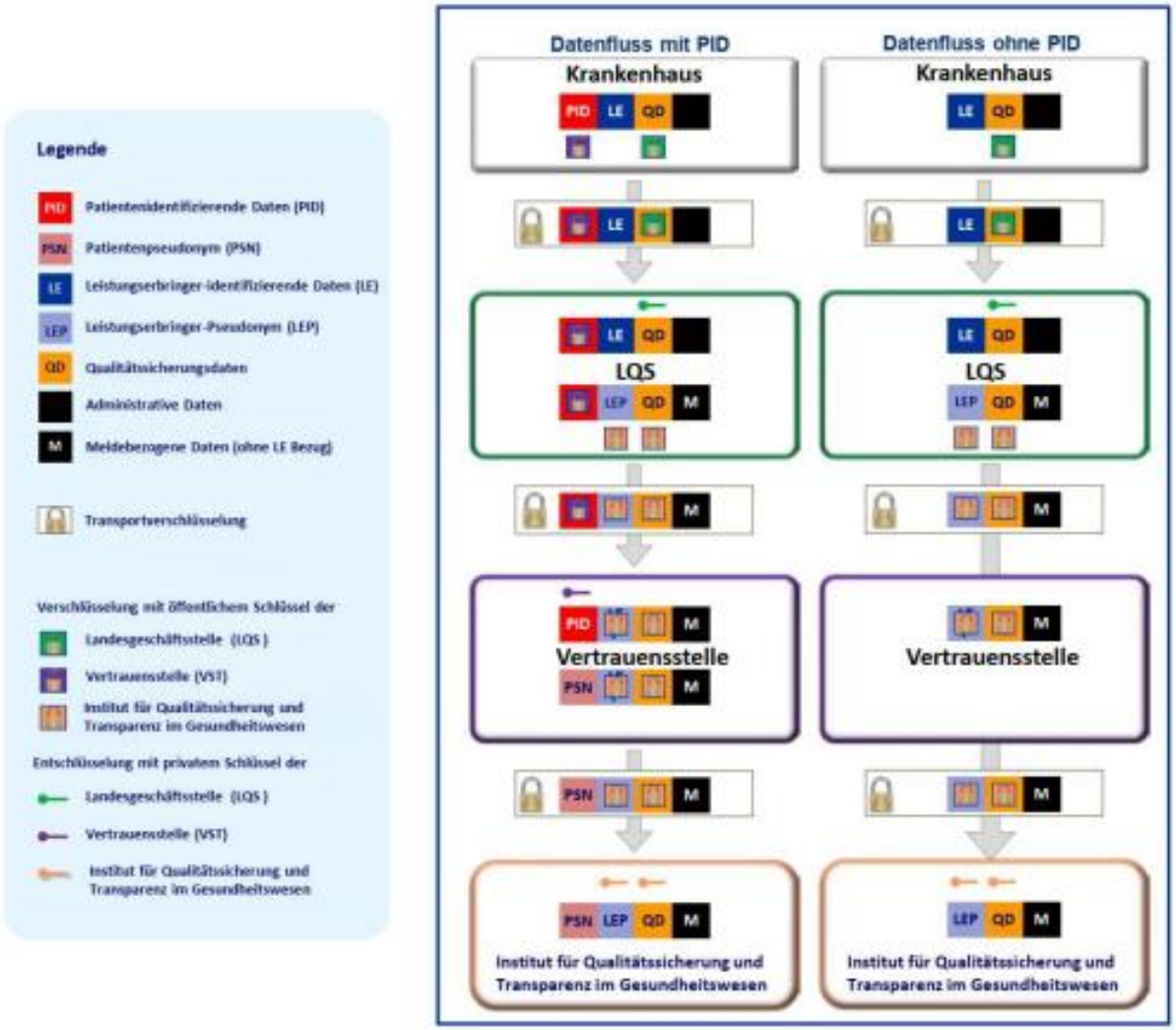
§ 19 Datenschutz und Schweigepflicht …

Anlage 3 Verfahren mit Follow-up

§ 4 Aufgaben im Krankenhaus

(5) Die Krankenhäuser übermitteln standortbezogen unverzüglich gemäß dem bundeseinheitlich vorgegebenen XML-Datenexportformat die auf der Grundlage der Spezifikation erfassten und geprüften sowie nach Absatz 4 verschlüsselten Daten gemäß Anhang 2 (Datenflussmodell) an die auf Landesebene beauftragte Stelle

G-BA Qesü-RL Anlage 3 Datenflussmodell



Sozialgesetzbuch (SGB) Erstes Buch (I) - Allgemeiner Teil – (Artikel I des Gesetzes vom 11. Dezember 1975, BGBl. I S. 3015)

Zuletzt geändert durch Art. 5 G v. 14.8.2017 I 3214

§ 36 Handlungsfähigkeit

(1) Wer das fünfzehnte Lebensjahr vollendet hat, kann Anträge auf Sozialleistungen stellen und verfolgen sowie Sozialleistungen entgegennehmen. …

§ 36a Elektronische Kommunikation

(1) Die Übermittlung elektronischer Dokumente ist zulässig, soweit der Empfänger hierfür einen Zugang eröffnet.

(2) Eine durch Rechtsvorschrift angeordnete Schriftform kann, … durch die elektronische Form ersetzt werden. …

2. bei Anträgen und Anzeigen durch Versendung eines elektronischen Dokuments an die Behörde mit der Versandart nach § 5 Absatz 5 des De-Mail-Gesetzes;

SGB V

Sozialgesetzbuch (SGB) Fünftes Buch (V) - Gesetzliche Krankenversicherung - (Artikel 1 des Gesetzes v. 20. Dezember 1988, BGBl. I S. 2477)

Zuletzt geändert durch Art. 4 G v. 17.8.2017 I 3214

§ 291 Elektronische Gesundheitskarte als Versicherungsnachweis

§ 291a Elektronische Gesundheitskarte und Telematikinfrastruktur

(4) Zum Zwecke des Erhebens, Verarbeitens oder Nutzens mittels der elektronischen Gesundheitskarte dürfen, soweit es zur Versorgung der Versicherten erforderlich ist, auf Daten

1. nach Absatz 2 Satz 1 Nr. 1 ausschließlich

a) Ärzte …

d) Personen, die

…

bb) in einem Krankenhaus als berufsmäßige Gehilfen … zugreifen

SGB V

(5) Das Erheben, Verarbeiten und Nutzen von Daten mittels der elektronischen Gesundheitskarte in den Fällen des Absatzes 3 Satz 1 ist nur mit dem Einverständnis der Versicherten zulässig. Durch technische Vorkehrungen ist zu gewährleisten, dass … der Zugriff … nur durch Autorisierung der Versicherten möglich ist.

§ 291d Integration offener Schnittstellen in informationstechnische Systeme, Verordnungsermächtigung

(1) In informationstechnische Systeme, die zum Erheben, Verarbeiten und Nutzen von personenbezogenen Patientendaten eingesetzt werden in …

3. Krankenhäusern,

sind offene und standardisierte Schnittstellen zur systemneutralen Archivierung von Patientendaten sowie zur Übertragung von Patientendaten bei einem Systemwechsel zu integrieren. Die Integration der Schnittstellen muss spätestens zwei Jahre, … erfolgt sein.

§ 291f Übermittlung elektronischer Briefe in der vertragsärztlichen Versorgung

(2) Das Nähere, insbesondere über Inhalt und Struktur des elektronischen Briefs, zur Abrechnung, zu Regelungen, die eine nicht bedarfsgerechte Mengenausweitung vermeiden, und Einzelheiten zu den Sicherheitsmaßnahmen, regelt die Kassenärztliche Bundesvereinigung im Benehmen mit dem Spitzenverband Bund der Krankenkassen und der Gesellschaft für Telematik in einer Richtlinie.

§ 299 Datenerhebung, -verarbeitung und -nutzung für Zwecke der Qualitätssicherung

(1) Die an der vertragsärztlichen Versorgung teilnehmenden Ärzte, zugelassenen Krankenhäuser und übrigen Leistungserbringer gemäß § 135a Absatz 2 sind befugt und verpflichtet, personen- oder einrichtungsbezogene Daten der Versicherten und der Leistungserbringer für Zwecke der Qualitätssicherung … zu erheben …

Die Richtlinien und Beschlüsse sowie Vereinbarungen nach Satz 1 haben darüber hinaus sicherzustellen, dass

1. in der Regel die Datenerhebung auf eine Stichprobe der betroffenen Patienten begrenzt wird und die versichertenbezogenen Daten pseudonymisiert werden,

(2) Das Verfahren zur Pseudonymisierung der Daten wird durch die an der vertragsärztlichen Versorgung teilnehmenden Ärzte und übrigen Leistungserbringer gemäß § 135a Absatz 2 angewendet.

§ 307 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer entgegen § 291a Abs. 8 Satz 1 eine dort genannte Gestattung verlangt oder mit dem Inhaber der Karte eine solche Gestattung vereinbart.

(1a) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig entgegen § 291b Absatz 6 Satz 2 und 4 eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig vornimmt.

(1b) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig entgegen § 291b Absatz 8 Satz 2 einer verbindlichen Anweisung nicht, nicht vollständig oder nicht rechtzeitig Folge leistet.

§ 307b Strafvorschriften

(1) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer entgegen § 291a Absatz 4 Satz 1 oder Absatz 5a Satz 1 erster Halbsatz oder Satz 2 auf dort genannte Daten zugreift.

(2) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen Anderen zu bereichern oder einen Anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu drei Jahren oder Geldstrafe.

SGB VIII

Sozialgesetzbuch (SGB) - Achtes Buch (VIII) - Kinder- und Jugendhilfe –

(Artikel 1 des Gesetzes v. 26. Juni 1990, BGBl. I S. 1163)

zuletzt geändert durch Art. 10 Abs. 10 G v. 30.10.2017 I 3618

Viertes Kapitel

Schutz von Sozialdaten

§ 61 Anwendungsbereich

§ 62 Datenerhebung

§ 63 Datenspeicherung

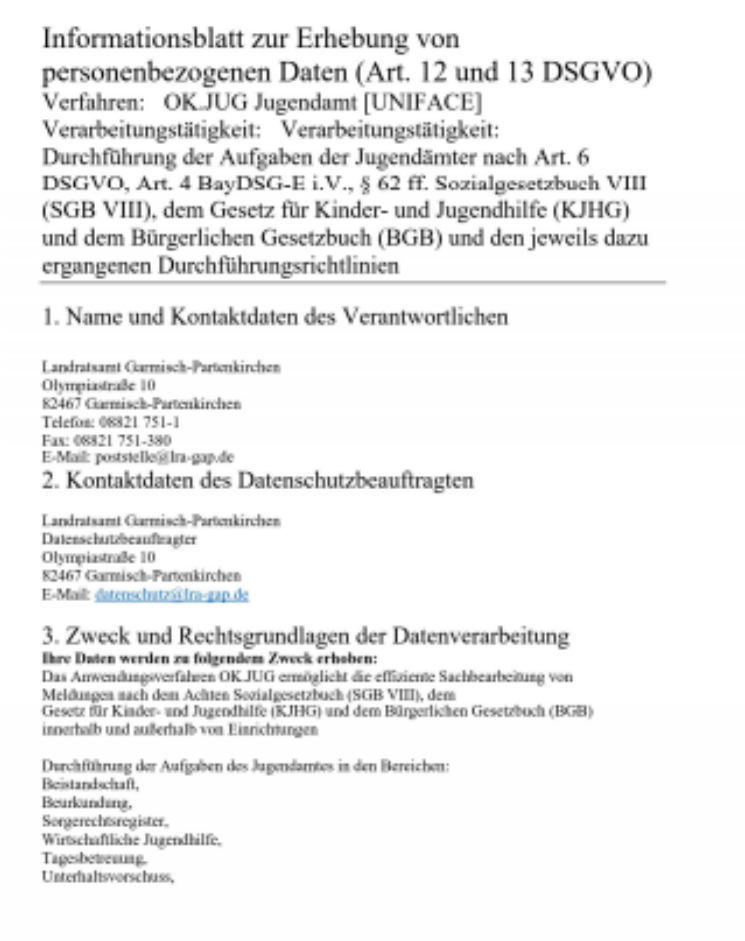
§ 64 Datenübermittlung und -nutzung

§ 65 Besonderer Vertrauensschutz in der persönlichen und erzieherischen Hilfe

SGB VIII

§ 62 Datenerhebung
§ 63 Datenspeicherung
§ 64 Datenübermittlung und -nutzung

Beispiel für den Einfluss der EU-DSGVO:
Informationspflichten Jugendamt GAP



Informationsblatt zur Erhebung von personenbezogenen Daten (Art. 12 und 13 DSGVO)

Verfahren: OK.JUG Jugendamt [UNIFACE]
Verarbeitungstätigkeit: Verarbeitungstätigkeit:
Durchführung der Aufgaben der Jugendämter nach Art. 6 DSGVO, Art. 4 BayDSG-E i.V., § 62 ff. Sozialgesetzbuch VIII (SGB VIII), dem Gesetz für Kinder- und Jugendhilfe (KJHG) und dem Bürgerlichen Gesetzbuch (BGB) und den jeweils dazu ergangenen Durchführungsrichtlinien

1. Name und Kontaktdaten des Verantwortlichen

Landratsamt Garmisch-Partenkirchen
Olympiastraße 10
82467 Garmisch-Partenkirchen
Telefon: 08821 751-1
Fax: 08821 751-380
E-Mail: poststelle@lra-gap.de

2. Kontaktdaten des Datenschutzbeauftragten

Landratsamt Garmisch-Partenkirchen
Datenschutzbeauftragter
Olympiastraße 10
82467 Garmisch-Partenkirchen
E-Mail: datenschutz@lra-gap.de

3. Zweck und Rechtsgrundlagen der Datenverarbeitung

Ihre Daten werden zu folgendem Zweck erhoben:
Das Anwendungsverfahren OK.JUG ermöglicht die effiziente Sachbearbeitung von Meldungen nach dem Achten Sozialgesetzbuch (SGB VIII), dem Gesetz für Kinder- und Jugendhilfe (KJHG) und dem Bürgerlichen Gesetzbuch (BGB) innerhalb und außerhalb von Einrichtungen

Durchführung der Aufgaben des Jugendamtes in den Bereichen:
Beistandschaft,
Beurkundung,
Sorgerechtsregister,
Wirtschaftliche Jugendhilfe,
Tagesbetreuung,
Unterhaltsvorschuss,

Rechtliche Grundlagen 2: Kaufmännisch

- ✓ Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)
- ✓ Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)
- ✓ Handelsgesetzbuch (HGB)
- ✓ Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)
- ✓ Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSiG)
- ✓ Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr (EU-DSGVO)
- ✓ Bundesdatenschutzgesetz (BDSG)

GoBD

Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)

Allgemeines

1. Die betrieblichen Abläufe in den Unternehmen werden ganz oder teilweise unter Einsatz von Informations- und KommunikationsTechnik abgebildet.

2. Auch die nach außersteuerlichen oder steuerlichen Vorschriften zu führenden Bücher und sonst erforderlichen Aufzeichnungen werden in den Unternehmen zunehmend in elektronischer Form geführt (z. B. als Datensätze). Darüber hinaus werden in den Unternehmen zunehmend die aufbewahrungspflichtigen Unterlagen in elektronischer Form (z. B. als elektronische Dokumente) aufbewahrt.

1.3 Aufbewahrung von Unterlagen zu Geschäftsvorfällen und von solchen Unterlagen, die zum Verständnis und zur Überprüfung der für die Besteuerung gesetzlich vorgeschriebenen Aufzeichnungen von Bedeutung sind

5. Neben den außersteuerlichen und steuerlichen Büchern, Aufzeichnungen und Unterlagen zu Geschäftsvorfällen sind alle Unterlagen aufzubewahren, die zum Verständnis und zur Überprüfung der für die Besteuerung gesetzlich vorgeschriebenen Aufzeichnungen im Einzelfall von Bedeutung sind …

   Dazu zählen neben Unterlagen in Papierform auch alle Unterlagen in Form von Daten, Datensätzen und elektronischen Dokumenten, die dokumentieren, dass die Ordnungsvorschriften umgesetzt und deren Einhaltung überwacht wurde. Nicht aufbewahrungspflichtig sind z. B. reine Entwürfe von Handels- oder Geschäftsbriefen, sofern diese nicht tatsächlich abgesandt wurden.

Form, Umfang und Inhalt dieser im Sinne der Rzn. 3 bis 5 nach außersteuerlichen und steuerlichen Rechtsnormen aufzeichnungs- und aufbewahrungspflichtigen Unterlagen

(Daten, Datensätze sowie Dokumente in elektronischer oder Papierform) und der zu ihrem Verständnis erforderlichen Unterlagen werden durch den Steuerpflichtigen bestimmt.

Eine abschließende Definition der aufzeichnungs- und aufbewahrungspflichtigen Aufzeichnungen und Unterlagen ist nicht Gegenstand der nachfolgenden Ausführungen.

Die Finanzverwaltung kann diese Unterlagen nicht abstrakt im Vorfeld für alle Unternehmen abschließend definieren, weil die betrieblichen Abläufe, … zu unterschiedlich sind.

GoBD

1.5 Führung von Büchern und sonst erforderlichen Aufzeichnungen auf Datenträgern

10. Technische Vorgaben oder Standards (z. B. zu Archivierungsmedien oder Kryptografieverfahren) können angesichts der rasch fortschreitenden Entwicklung und der ebenfalls notwendigen Betrachtung des organisatorischen Umfelds nicht festgelegt werden.

Im Zweifel ist über einen Analogieschluss festzustellen, ob die Ordnungsvorschriften eingehalten wurden, z. B. bei einem Vergleich zwischen handschriftlich geführten Handelsbüchern und Unterlagen in Papierform, die in einem verschlossenen Schrank aufbewahrt werden, einerseits und elektronischen Handelsbüchern und Unterlagen, die mit einem elektronischen Zugriffschutz gespeichert werden, andererseits.

3. Allgemeine Anforderungen

22. Die Ordnungsmäßigkeit elektronischer Bücher und sonst erforderlicher elektronischer Aufzeichnungen im Sinne der Rzn. 3 bis 5 ist nach den gleichen Prinzipien zu beurteilen wie die Ordnungsmäßigkeit bei manuell erstellten Büchern oder Aufzeichnungen.

26. Demnach sind … die folgenden Anforderungen zu beachten: • Grundsatz der Nachvollziehbarkeit und Nachprüfbarkeit (siehe 3.1), • Grundsätze der Wahrheit, Klarheit und fortlaufenden Aufzeichnung (siehe unter 3.2):

- ✓ Vollständigkeit (siehe unter 3.2.1),
- ✓ Richtigkeit (siehe unter 3.2.2),
- ✓ zeitgerechte Buchungen und Aufzeichnungen (siehe unter 3.2.3),
- ✓ Ordnung (siehe unter 3.2.4), Unveränderbarkeit (siehe unter 3.2.5)

GoBD

27. Diese Grundsätze müssen während der Dauer der Aufbewahrungsfrist nachweisbar erfüllt werden und erhalten bleiben.
28. Nach § 146 Absatz 6 AO gelten die Ordnungsvorschriften auch dann, wenn der Unternehmer elektronische Bücher und Aufzeichnungen führt, die für die Besteuerung von Bedeutung sind, ohne hierzu verpflichtet zu sein.
29. Der Grundsatz der Wirtschaftlichkeit rechtfertigt es nicht, dass Grundprinzipien der Ordnungsmäßigkeit verletzt und die Zwecke der Buchführung erheblich gefährdet werden. Die zur Vermeidung einer solchen Gefährdung erforderlichen Kosten muss der Steuerpflichtige genauso in Kauf nehmen wie alle anderen Aufwendungen, die die Art seines Betriebes mit sich bringt (BFH-Urteil vom 26. März 1968, BStBl II S. 527).

3.2.5 Unveränderbarkeit (§ 146 Absatz 4 AO, § 239 Absatz 3 HGB)

58. Eine Buchung oder eine Aufzeichnung darf nicht in einer Weise verändert werden, dass der ursprüngliche Inhalt nicht mehr feststellbar ist. Auch solche Veränderungen dürfen nicht vorgenommen werden, deren Beschaffenheit es ungewiss lässt, ob sie ursprünglich oder erst später gemacht worden sind (§ 146 Absatz 4 AO, § 239 Absatz 3 HGB)

4.1 Belegsicherung

67. Die Belege in Papierform oder in elektronischer Form sind zeitnah, d. h. möglichst unmittelbar nach Eingang oder Entstehung gegen Verlust zu sichern (vgl. zur zeitgerechten Belegsicherung unter 3.2.3, vgl. zur Aufbewahrung unter 9.)

7. Datensicherheit

103.Der Steuerpflichtige hat sein DV-System gegen Verlust (z. B. Unauffindbarkeit, Vernichtung, Untergang und Diebstahl) zu sichern und gegen unberechtigte Eingaben und Veränderungen (z. B. durch Zugangs- und Zugriffskontrollen) zu schützen.

8. Unveränderbarkeit, Protokollierung von Änderungen

107.107 Nach § 146 Absatz 4 AO darf eine Buchung oder Aufzeichnung nicht in einer Weise verändert werden, dass der ursprüngliche Inhalt nicht mehr feststellbar ist. Auch solche Veränderungen dürfen nicht vorgenommen werden, deren Beschaffenheit es ungewiss lässt, ob sie ursprünglich oder erst später gemacht worden sind.

110.Die Unveränderbarkeit der Daten, Datensätze, elektronischen Dokumente und elektronischen Unterlagen (vgl. Rzn. 3 bis 5) kann sowohl hardwaremäßig (z. B. unveränderbare und fälschungssichere Datenträger) als auch softwaremäßig (z. B. Sicherungen, Sperren, Festschreibung, Löschmerker, automatische Protokollierung, Historisierungen, Versionierungen) als auch organisatorisch (z. B. mittels Zugriffsberechtigungskonzepten) gewährleistet werden. Die Ablage von Daten und elektronischen Dokumenten in einem Dateisystem erfüllt die Anforderungen der Unveränderbarkeit regelmäßig nicht, soweit nicht zusätzliche Maßnahmen ergriffen werden, die eine Unveränderbarkeit gewährleisten

119. Sind aufzeichnungs- und aufbewahrungspflichtige Daten, Datensätze, elektronische Dokumente und elektronische Unterlagen im Unternehmen entstanden oder dort eingegangen, sind sie auch in dieser Form aufzubewahren und dürfen vor Ablauf der Aufbewahrungsfrist nicht gelöscht werden. Sie dürfen daher nicht mehr ausschließlich in ausgedruckter Form aufbewahrt werden und müssen für die Dauer der Aufbewahrungsfrist unveränderbar erhalten bleiben (z. B. per E-Mail eingegangene Rechnung im PDF-Format oder eingescannte Papierbelege).

10.1 Verfahrensdokumentation

… erstellen (gilt auch für gescannte Dokumente)

Abgabenordnung

Schreiben des Bundesministeriums der Finanzen an die obersten Finanzbehörden der Länder vom 7. November 1995 - IV A 8 - S 0316 - 52/95- BStBl 1995 I S. 738

Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)

Anwendungsbereich

a) Die nach steuerlichen Vorschriften zu führenden Bücher … können … auf Datenträgern geführt werden, soweit diese … den Grundsätzen ordnungsmäßiger Buchführung (GoB) entspricht; …

b) Die Ordnungsmäßigkeit einer DV-gestützten Buchführung ist grundsätzlich nach den gleichen Prinzipien zu beurteilen wie die einer manuell erstellten Buchführung. …

V. Datensicherheit

(Tz. 5 der GoBS)

Zu sichern und zu schützen sind neben den genannten "Informationen" auch die Änderungen der Tabellen- und Stammdaten. Ihre Sicherung ist ebenso von Bedeutung wie die Sicherung anderer Programm- und Stammdaten. …

VI. Dokumentation und Prüfbarkeit

(Tz. 6 der GoBS)

a) Für jedes DV-gestützte Buchführungssystem ist eine Dokumentation zu erstellen (Verfahrensdokumentation).

VIII. Wiedergabe der auf Datenträgern geführten Unterlagen (Tz. 8 der GoBS)

a) Der Buchführungspflichtige, der aufzubewahrende Unterlagen nur in Form einer Wiedergabe auf einem Datenträger vorlegen kann, ist verpflichtet, auf seine Kosten diejenigen Hilfsmittel zur Verfügung zu stellen, die erforderlich sind, um die Unterlagen lesbar zu machen; auf Verlangen der Finanzbehörde hat er auf seine Kosten die Unterlagen unverzüglich ganz oder teilweise auszudrucken bzw. lesbare Reproduktionen beizubringen (vgl. zu II.).

Handelsgesetzbuch

§ 238 Buchführungspflicht

(1) Jeder Kaufmann ist verpflichtet, Bücher zu führen und in diesen seine Handelsgeschäfte und die Lage seines Vermögens nach den Grundsätzen ordnungsmäßiger Buchführung ersichtlich zu machen. Die Buchführung muß so beschaffen sein, daß sie einem sachverständigen Dritten innerhalb angemessener Zeit einen Überblick über die Geschäftsvorfälle und über die Lage des Unternehmens vermitteln kann. Die Geschäftsvorfälle müssen sich in ihrer Entstehung und Abwicklung verfolgen lassen.

(2) (2) Der Kaufmann ist verpflichtet, eine mit der Urschrift übereinstimmende Wiedergabe der abgesandten Handelsbriefe (Kopie, Abdruck, Abschrift oder sonstige Wiedergabe des Wortlauts auf einem Schrift-, Bild- oder anderen Datenträger) zurückzubehalten.

§ 257 Aufbewahrung von Unterlagen –Aufbewahrungsfristen

1. Jeder Kaufmann ist verpflichtet, die folgenden Unterlagen geordnet aufzubewahren:
   1. Handelsbücher, Inventare, Eröffnungsbilanzen, Jahresabschlüsse, Einzelabschlüsse nach § 325 Abs. 2a, Lageberichte, Konzernabschlüsse, Konzernlageberichte sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen,
   2. die empfangenen Handelsbriefe,
   3. Wiedergaben der abgesandten Handelsbriefe,
   4. Belege für Buchungen in den von ihm nach § 238 Abs. 1 zu führenden Büchern (Buchungsbelege).
2. Handelsbriefe sind nur Schriftstücke, die ein Handelsgeschäft betreffen. …

Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)

Vom 27. April 1998

Die am meisten beachtete Maßnahme ist die Einfügung des § 91 Absatz 2 Aktiengesetz. Danach hat der Vorstand geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.

Der § 91 Absatz 2 Aktiengesetz gilt zunächst nur für Gesellschaften, die dem Aktiengesetz unterliegen.

Deshalb ein Blick in das Aktiengesetz

Aktiengesetz

§ 91 Organisation. Buchführung

(1) Der Vorstand hat dafür zu sorgen, daß die erforderlichen Handelsbücher geführt werden.

(2) Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.

Aktiengesetz § 91 (2) Anleitung

Ganzheitliches Risikomanagement als Lösungsansatz

- ✓ Risikoidentifikation, die Risikoanalyse und nachfolgende Bewertung, die Steuerung der Risiken als Konsequenz der Bewertung und die Überwachung und Kontrolle des Erfolges.

- ✓ □ Der Anspruch des KonTraG ist es, dass alle Unternehmensrisiken erfasst werden. Quelle: http://www.risikomanagement.info/Risikomanagement-und-das-Gesetz-zur-Kontrolle-undTransparenz-im-Unternehme.309.0.html

Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG)

Zuletzt geändert durch Art. 1 G v. 23.6.2017 I 1885

§ 1 Bundesamt für Sicherheit in der Informationstechnik

Der Bund unterhält ein Bundesamt für Sicherheit in der Informationstechnik (Bundesamt) als Bundesoberbehörde. Das Bundesamt ist zuständig für die Informationssicherheit auf nationaler Ebene. Es untersteht dem Bundesministerium des Innern.

§ 8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen

(1) Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.

§ 8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen

(3) Die Betreiber Kritischer Infrastrukturen haben mindestens alle zwei Jahre die Erfüllung der Anforderungen nach Absatz 1 auf geeignete Weise nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Die Betreiber übermitteln dem Bundesamt die Ergebnisse der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel. Das Bundesamt kann die Vorlage der Dokumentation, die der Überprüfung zugrunde gelegt wurde, verlangen. Es kann bei Sicherheitsmängeln im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen

BSiG

§ 8b Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen

(1) Das Bundesamt ist die zentrale Meldestelle für Betreiber Kritischer Infrastrukturen in Angelegenheiten der Sicherheit in der Informationstechnik.

(3) Die Betreiber Kritischer Infrastrukturen haben dem Bundesamt binnen sechs Monaten nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 eine Kontaktstelle für die von ihnen betriebenen Kritischen Infrastrukturen zu benennen. Die Betreiber haben sicherzustellen, dass sie hierüber jederzeit erreichbar sind. Die Übermittlung von Informationen durch das Bundesamt nach Absatz 2 Nummer 4 erfolgt an diese Kontaktstelle.

§ 8b Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen

(4) Betreiber Kritischer Infrastrukturen haben die folgenden Störungen unverzüglich über die Kontaktstelle an das Bundesamt zu melden:

1.Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen geführt haben,

2. erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können.

BSiG – Definition „Kritische Infrastrukturen“

Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden

Sektoren	Branchen
Gesundheit	Medizinische Versorgung Arzneimittel und Impfstoffe Labore

Der Schwellenwert zur Identifikation kritischer Infrastrukturen wurde auf 30.000 vollstationäre Behandlungsfälle festgelegt. Gemäß BSI-KritisV haben Krankenhäuser künftig jeweils zum 31. März zu prüfen, ob sie diesen Schwellenwert erreichen oder überschreiten.

Ein Übergangszeitraum ist ausdrücklich nicht vorgesehen.

BSiG – Anforderungen

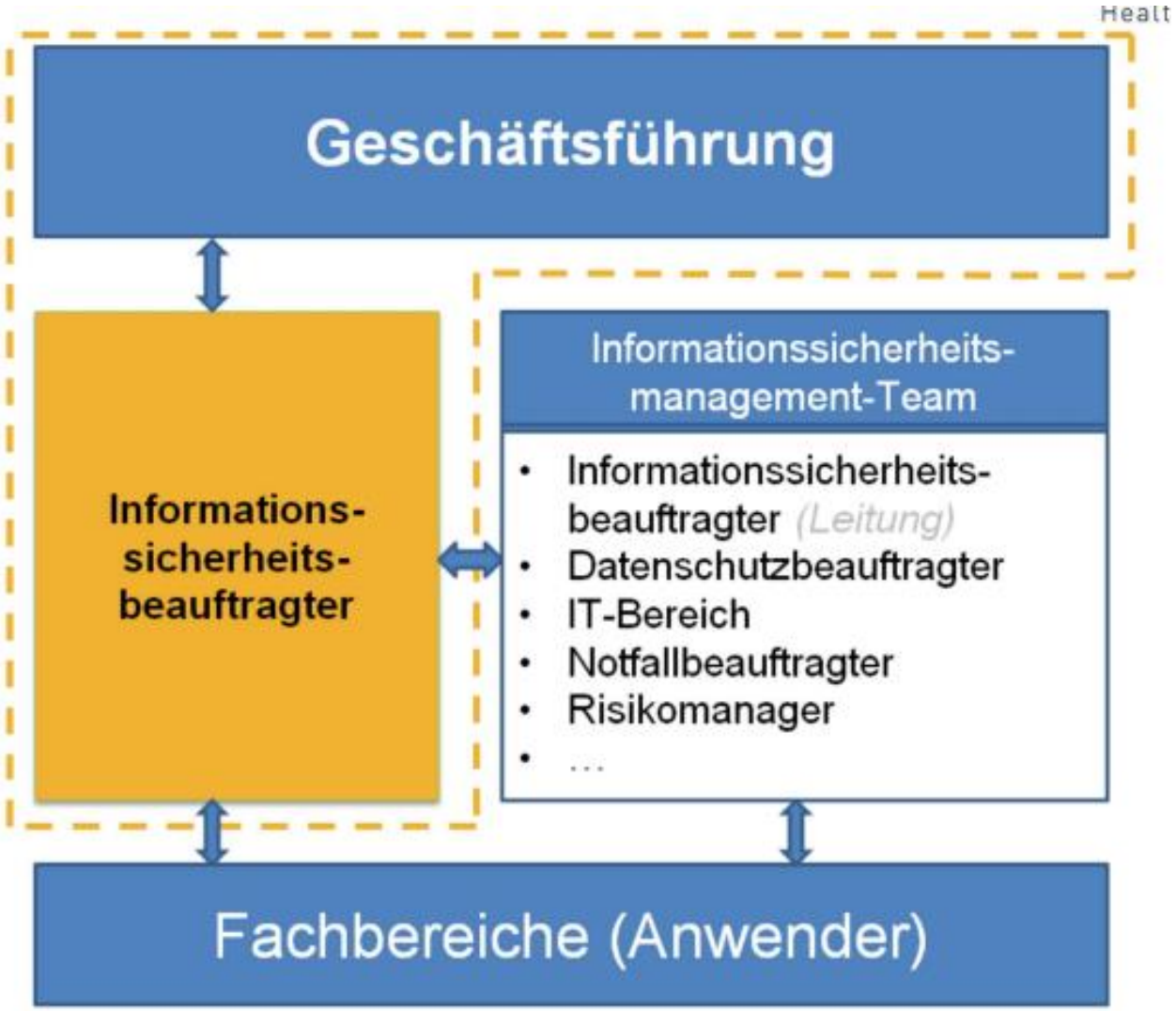
Maßnahmen bei Überschreitung des Schwellenwertes

- ✓ Registrierung als kritische Infrastruktur und Einrichtung Kontaktstelle
- ✓ Meldung von IT-Störungen an das BSI
- ✓ Umsetzung von Maßnahmen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse
- ✓ Die Schritte sind sofort umzusetzen, diese gelten ab dem 1.4. des Jahres, das auf die Überschreitung des Schwellenwertes folgt
- ✓ Der Nachweis der Umsetzung ist spätestens 2 Jahre nach Feststellung der Schwellenwertüberschreitung zu erbringen
- ✓ Ist der Schwellwert nur knapp unterschritten, sollten vorbereitende Maßnahmen getroffen werden, um ggf. im Folgejahr die dann sofort greifende Verpflichtung zur Umsetzung realisieren zu können

BSiG – Definition „Kritische Infrastrukturen“

- ✓ Für Krankenhäuser, welche die Kriterien kritischer Infrastruktur zwei Jahre in Folge erfüllen, entsteht eine Nachweispflicht zur Umsetzung geeigneter organisatorischer und technischer Vorkehrungen zur Vermeidung von Störungen der informationstechnischen Systeme.
- ✓ Wesentliches Ziel der festgelegten Informationspflichten ist der Austausch von für IT-Sicherheit relevanten Informationen zwischen den Betreibern kritischer Infrastrukturen und dem BSI.
- ✓ Es muss ein Prozess beschrieben werden, wie mit Vorfällen im Bereich der IT-Sicherheit umgegangen wird und wann eine Meldung sinnvoll bzw. notwendig ist.
- ✓ §10 (2) BSiG stellt es Betreibern kritischer Infrastrukturen sowie deren Branchenverbänden frei, „branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach Absatz 1“ vorzuschlagen
- ✓ Der Aufbau eines ISMS wird als Basis für die Umsetzung angesehen

BSiG – Umsetzung Aufbauorg. IT-Sicherheit



BSiG - Anforderungen

Technische und organisatorische Schutzmaßnahmen

- ✓ Absicherungsmaßnahmen, wenn IT Einfluss auf die Dienstleistung hat
- ✓ Erhalt von Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit
- ✓ Prävention
- ✓ Untersuchung und Behebung von Störungen

BSiG - Anforderungen

„Der Stand der Technik“

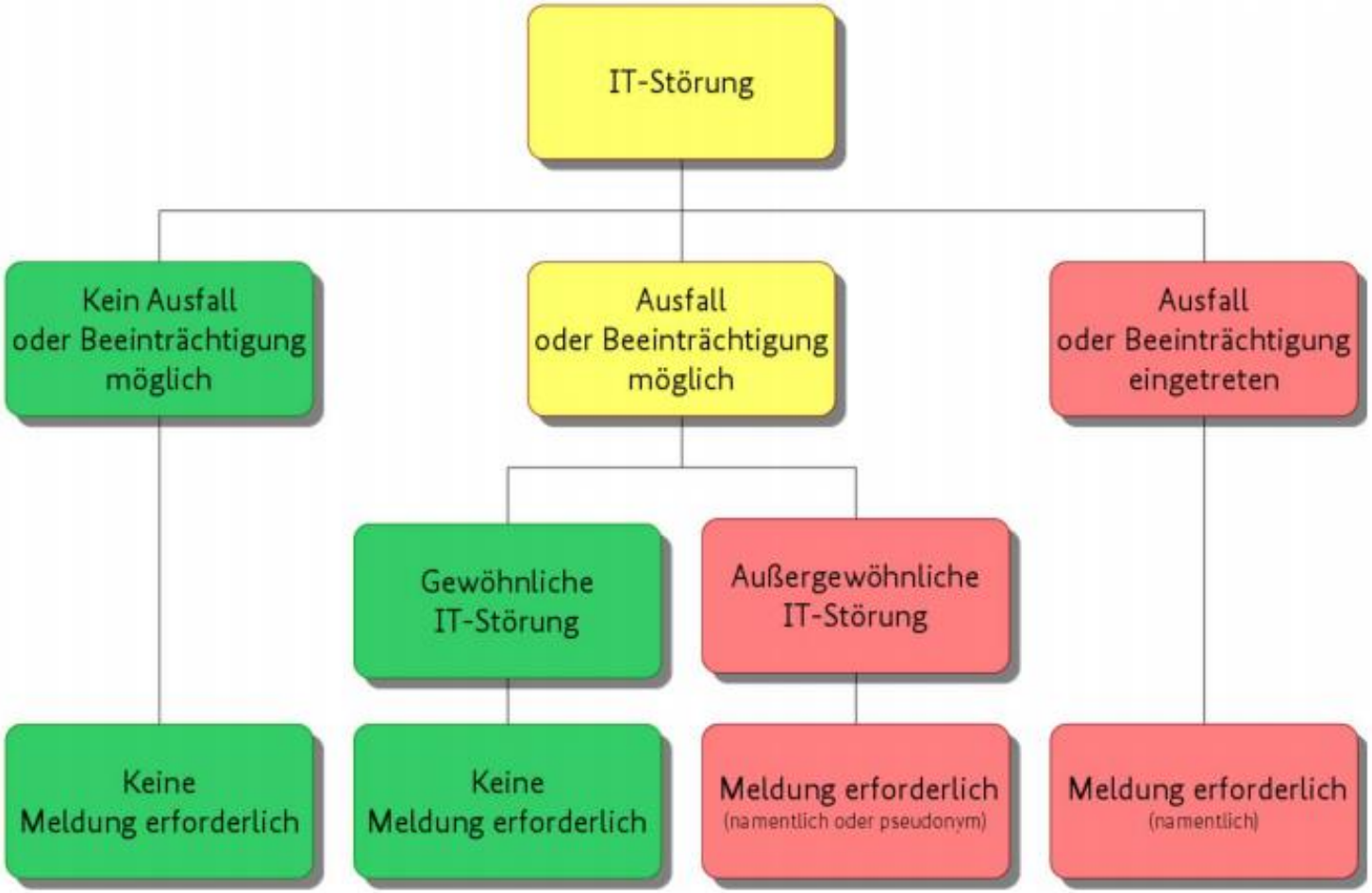
- ✓ Keine Legaldefinition (Flexibilität) = Unbestimmter Rechtsbegriff
- ✓ „Soll-“Vorschrift
- ✓ Erarbeitung durch die Betreiber selbst oder deren Branchenverbände
- ✓ Zweijährlich Audit / Prüfung / Zertifizierung
- ✓ Nachweispflicht gegenüber dem BSI

BSiG - Anforderungen

Warn-, Hinweis- und Meldepflichten

- ✓ Erhebliche Störungen IT-System, Komponenten oder Prozesse, erheblich sind:
  - Gezielte Angriffe
  - Neuer Modus Operandi
  - Unerwartete Vorkommnisse
  - Deutlich erhöhter Ressourcenaufwand
- ✓ „Störung“ = eingesetzte Technik kann ihre Funktion nicht mehr oder nicht mehr vollständig erfüllen (auch: erfolglose Angriffe)

BSiG – Meldepflichtige Störungen



§ 14 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 8a … eine dort genannte Vorkehrung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig trifft,
2. einer vollziehbaren Anordnung nach § 8a Absatz 3 Satz 5 zuwiderhandelt,
3. entgegen § 8b Absatz 3 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 10 Absatz 1 Satz 1 eine Kontaktstelle nicht oder nicht rechtzeitig benennt,
4. entgegen § 8b Absatz 4 Satz 1 Nummer 2 eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,
5. entgegen § 8c Absatz 1 Satz 1 eine dort genannte Maßnahme nicht trifft,
6. entgegen § 8c Absatz 3 Satz 1 eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig vornimmt oder

§ 14 Bußgeldvorschriften

7. einer vollziehbaren Anordnung nach § 8c Absatz 4

a) Nummer 1 oder

b) Nummer 2

zuwiderhandelt.

(2) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nummer 2 Buchstabe b mit einer Geldbuße bis zu hunderttausend Euro, in den übrigen Fällen des Absatzes 1 mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.

VERORDNUNG (EU) 2016/679

DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 27.04.2016

zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

Artikel 1

Gegenstand und Ziele

(1) Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.

(2) Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.

EU-DSGVO

- ✓ Sicherheit der Verarbeitung Art. 32 DS-GVO
  - ➢ Risikobewertung
  - ➢ Technische und organisatorische Maßnahmen
  - ➢ Nachweis der Konformität
- ✓ Videoüberwachung
- ✓ Datenschutz-Folgeabschätzung
- ✓ Verzeichnis von Verarbeitungstätigkeiten Art. 30 DS-GVO
  - ➢ Inhalt des Verzeichnisses für Auftragsdatenverarbeiter (Art. 30 Abs. 2)
- ✓ Besondere Kategorien personenbezogener Daten - Art. 9 DS-GVO

EU-DSGVO

- ✓ Geldbußen und Sanktionen – Art. 83 und 84 DS-GVO
- ✓ Umgang mit Datenpannen – Art. 33 und 34 DS-GVO
- ✓ Einwilligung nach der DS-GVO
  - ➢ Nachweis des Vorliegens einer Einwilligung
  - ➢ Unwirksame Einwilligung – Bussgeld
  - ➢ Bestandsgarantie von Einwilligungen
  - ➢ Frist für Fortgeltung

EU-DSGVO

- ✓ Auftragsverarbeitung nach der DS-GVO - Art. 28
  - ➢ Vertrag mit Maßnahmen zur Sicherheit
  - ➢ Subunternehmer-Einsatz
  - ➢ Neue Verantwortlichkeiten und Pflichten
  - ➢ Haftungsregelungen
  - ➢ Wartung und Fernzugriffe
- ✓ Datenpannen und Folgen bei Verstößen
- ✓ Datenübermittlungen in Drittstaaten nach der DS-GVO

Planung der Umsetzung

Voruntersuchung	Herausforderung
Bestandsaufnahme bestehender Datenschutzstrukturen	Mittel
Verzeichnis aller Verarbeitungsvorgänge	Hoch
Prüfung der Rechtmäßigkeitsgrundlagen	Hoch
Gap-Analyse zwischen Ist-Zustand und Soll- Zustand	Mittel
Entwicklung von Lösungsoptionen	Hoch
Einbindung des Datenschutzbeauftragten	Niedrig

Umsetzung

Umsetzungsphase	Priorität	Herausforderung
Risikoanalyse DSGVO	Hoch	Hoch
Datenschutzkommunikation im Unternehmen	Mittel	Mittel
Schulung und Sensibilisierung der Mitarbeiter	Hoch	Mittel
Einführung eines DMS	Hoch	Hoch
· Zweckfestlegung und -änderung	Hoch	Mittel
· Löschkonzepte	Hoch	Mittel
· Datenschutz-Folgenabschätzung	Hoch	Hoch
· Sicherheit der Verarbeitung	Hoch	Hoch
· Aktualität des Verarbeitungsverzeichnisses	Mittel	Mittel
· Sicherstellung der Betroffenenrechte	Hoch	Hoch

Umsetzung

· **Kommunikation mit der Aufsichtsbehörde**	**Niedrig**	**Niedrig**
· Datentransfers in Drittländer	Mittel	Hoch
· Dokumentation sämtlicher relevanter Prozesse	Hoch	Hoch
· Privacy by design and by default	Mittel	Hoch
· Big data	Mittel	Hoch
Anpassung der Auftragsverarbeitungen	Hoch	Hoch
Vereinbarung über gemeinsame Verantwortliche	Mittel	Mittel
Einrichtung eines Beschwerdemanagements	Hoch	Hoch
Überprüfung bestehender Verträge	Hoch	Mittel
Einwilligungsmanagement	Hoch	Hoch

EU-DSGVO - Dokumente im Datenschutz

- ✓ Richtlinie zur Datenschutzorganisation
- ✓ Ab 10. Mitarbeiter:
  - ➢ Bestellung des DSB / Dienstvertrag
  - ➢ Benennung des DSB beim Landesbeauftragten
  - ➢ Verfahrensanweisung zur Einbindung des DSB
- ✓ Übersicht der Rollen und Verantwortlichkeiten
- ✓ Verzeichnis der Verarbeitungstätigkeiten (VVT)
- ✓ Checkliste zur Beachtung der Anforderungen an Privacy-by Design/ Privacy-by-Default

EU-DSGVO - Dokumente im Datenschutz

- ✓ Risikominimierung durch Datenschutz-Folgenabschätzung
- ✓ Verhaltensmaßnahmen bei einer Datenpanne
- ✓ Umgang mit personenbezogenen Daten/ Erlaubnistatbestände der DS-GVO
  - ➢ Dokumentation der Einwilligung je Betroffenem
  - ➢ Information über die Betroffenenrechte
- ✓ Kompatibilitätscheck bei Zweckänderung

EU-DSGVO Dokumente der IT-Sicherheit

- ✓ IT-Sicherheitsrichtlinie (Art. 32 EU-DSGVO)
- ✓ Prozessbeschreibungen (je Prozess, z. B. CRM, Personalbuchhaltung, Bewerbermanagement)
- ✓ Assetverwaltung (Liste Hardware/Software/schützenswerte Daten/externe Dienstleister)
- ✓ Change-Management (Erfassung von Änderungen mit Freigabe) Notfallhandbuch (resilience)
- ✓ Dokumentation Backup und Restore (Doku Restore-Übungen)

EU-DSGVO Dokumente der IT-Sicherheit

Erforderliche technische und organisatorische Maßnahmen:

- ✓ Zutrittskontrolle
- ✓ Zugangskontrolle
- ✓ Zugriffskontrolle
- ✓ Weitergabekontrolle
- ✓ Eingabekontrolle
- ✓ Auftragskontrolle
- ✓ Verfügbarkeitskontrolle
- ✓ Trennungskontrolle
- ✓ Belastbarkeit (resilience)
- ✓ Berücksichtigung des Stands der Technik
- ✓ Berücksichtigung des vom jeweiligen Verfahren ausgehenden Risikos der Beeinträchtigung von Persönlichkeits- und Freiheitsrechten bei der Planung und Umsetzung von technischen und organisatorischen Maßnahmen
- ✓ Kontrollprozesse (PDCA)

EU-DSGVO Dokumente der IT-Sicherheit

- ✓ Arbeitsanweisung zum Versand von Datenträgern und zur Verschlüsselung von Daten
- ✓ Arbeitsanweisung zum Passwortverfahren
- ✓ Arbeitsanweisung zur Erteilung von Auskünften im Personalbereich
- ✓ Arbeitsanweisung zur PC- und Laptop-Nutzung
- ✓ Arbeitsanweisung Telearbeit/Home-Office
- ✓ Arbeitsanweisung Internet- und E-Mail-Nutzung

EU-DSGVO Dokumente der IT-Sicherheit

Art. 32 Satz 1 Ziffer d)

- ✓ Verfahren zur regelmäßigen
  - Überprüfung,
  - Bewertung und
  - Evaluierung
- ✓ der Wirksamkeit der technischen und organisatorischen Maßnahmen

EU-DSGVO - Auftragsverarbeitungsvertrag

- ✓ Auftragsverarbeitungsvertrag (AVV je Vertragspartner)
  - ➢ Haftungsregelungen
  - ➢ Ggf. Abschluss/Erweiterung einer Vermögensschadenhaftpflichtversicherung
- ✓ Dokumentation der regelmäßigen Audits der Lieferanten/Dienstleister

EU-DSGVO Fazit Accountability

Die Erfüllung der in der EU-DSGVO geforderten Rechenschaftspflicht ist nur durch

- ✓ schlüssige und
- ✓ nachvollziehbare
- ✓ schriftliche Dokumentation hinsichtlich
- ✓ getroffener Maßnahmen und
- ✓ dazugehöriger Abwägungen möglich

Art. 93 Hohe Bußgelder von bis zu 2-4% des Konzernjahresumsatzes des vorvergangenen Jahres

Bundesdatenschutzgesetz (BDSG)

Ausfertigungsdatum: 30.06.2017 (Geltung ab 25.05.2018)

(Nachrangiges Gesetz gegenüber der EU-DSGVO, vorrangig im Bereich der Öffnungsklauseln)

§ 1 Anwendungsbereich des Gesetzes

(1)Dieses Gesetz gilt für die Verarbeitung personenbezogener Daten durch öffentliche Stellen des Bundes,

2. öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist …

Für nichtöffentliche Stellen gilt dieses Gesetz für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, es sei denn, die Verarbeitung durch natürliche Personen erfolgt zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten. …

Teil drei

§ 45 Anwendungsbereich

Die Vorschriften dieses Teils gelten für die Verarbeitung personenbezogener Daten durch die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten zuständigen öffentlichen Stellen, soweit sie Daten zum Zweck der Erfüllung dieser Aufgaben verarbeiten. Die öffentlichen Stellen gelten dabei als Verantwortliche.

Achtung Falle: Demnach gelten für nicht dem § 45 unterliegende Stellen nur die §§ 1-44!

§ 22 Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 zulässig

1. durch öffentliche und nichtöffentliche Stellen, wenn sie

a) erforderlich ist, um die aus dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte auszuüben und den diesbezüglichen Pflichten nachzukommen,

b) zum Zweck der Gesundheitsvorsorge, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- und Sozialbereich oder aufgrund eines Vertrags … mit einem Angehörigen eines Gesundheitsberufs erforderlich ist und diese Daten von … Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, … verarbeitet werden, oder …

§ 41 Anwendung der Vorschriften über das Bußgeld- und Strafverfahren

(1) Für Verstöße nach Artikel 83 Absatz 4 bis 6 der Verordnung (EU) 2016/679 gelten, soweit dieses Gesetz nichts anderes bestimmt, die Vorschriften des Gesetzes über Ordnungswidrigkeiten sinngemäß. Die §§ 17, 35 und 36 des Gesetzes über Ordnungswidrigkeiten finden keine Anwendung.

§ 42 Strafvorschriften

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein,

1. einem Dritten übermittelt oder
2. auf andere Art und Weise zugänglich macht und hierbei gewerbsmäßig handelt.

(2) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer personenbez. Daten, die nicht allgemein zugänglich sind,

1. ohne hierzu berechtigt zu sein, verarbeitet oder
2. durch unrichtige Angaben erschleicht und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

BDSG

§ 43 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 30 Absatz 1 ein Auskunftsverlangen nicht richtig behandelt oder

2. entgegen § 30 Absatz 2 Satz 1 einen Verbraucher nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.

(3) Gegen Behörden und sonstige öffentliche Stellen im Sinne des § 2 Absatz 1 werden keine Geldbußen verhängt.

5.2 Normen & Managementsysteme

- ✓ DIN EN 80001-1:2011-11 Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten - Teil 1: Aufgaben, Verantwortlichkeiten und Aktivitäten
- ✓ DIN ISO 27001:2013 Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen
- ✓ ISO/IEC 20000-1 Information technology - Service management - Part 1: Service management system requirements
- ✓ ISO/IEC 22301 (zuvor BS 25999)
- ✓ BSI Standard 100-4 Notfallmanagement
- ✓ ISO 31000 Risk management — Principles and guidelines
- ✓ DIN EN ISO 14971 Medical devices – Application of risk management to medical devices

DIN EN 80001-1:2011-11

Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten - Teil 1: Aufgaben, Verantwortlichkeiten und Aktivitäten

- ✓ Die Norm definiert Aufgaben, Verantwortlichkeiten und Aktivitäten, damit das Risikomanagement der IT-Netzwerke mit Medizinprodukten die Sicherheit, Effektivität sowie Daten- und Systemsicherheit einhält.
- ✓ Diese Norm gilt nach dem ersten In-Verkehr-Bringen, wenn ein oder mehrere Medizinprodukt(e) von der verantwortlichen Organisation erworben wurde und in ein IT-Netzwerk eingefügt werden soll(en).
- ✓ Diese Norm gilt, wenn es keinen Medizinprodukte-Hersteller gibt, der die Gesamtverantwortung für die Einhaltung der Schutzziele (keyproperties) des IT-Netzwerks, das ein Medizinprodukt beinhaltet, übernimmt.

DIN EN 80001-1:2011-11

- ✓ Die Norm richtet sich an verantwortliche Organisationen, Hersteller von Medizinprodukten und Anbieter sonstiger IT-Technologie.
- ✓ Sie gilt nicht für Anwendungen des persönlichen Gebrauchs, bei denen der Patient, der Bediener und die verantwortliche Organisation ein und dieselbe Person sind.
- ✓ Die Interpretation der Anforderungen insbesondere zu den Kapiteln 3.5 (ebenso 3.6) und 4.3.4 kann unterschiedlich ausfallen, je nachdem ob diese aus Sicht der verantwortlichen Organisation beziehungsweise Hersteller-Sicht formuliert wird.
- ✓ In diesem Zusammenhang ist eine wesentliche Frage die Einigung über eine Hol- beziehungsweise Bringschuld bei der Bereitstellung und Definition "wichtiger aktualisierter Informationen".

DIN EN 80001-1:2011-11

Anwendungsbereich

Diese internationale Norm ist eine Norm über einen PROZESS, der Maßnahmen und besonders das RISIKOMANAGEMENT umfasst, welches von der VERANTWORTLICHEN ORGANISATION und dem HERSTELLER gefordert werden, wenn MEDIZINPRODUKTE in ein Netzwerk eingebunden werden oder derartige Einbindungen verändert werden

DIN EN 80001-1:2011-11

Vier „wesentliche Merkmale“

- ✓ Sicherheit
- ✓ Leistungsfähigkeit
  - wirkungsvolle Behandlung des Patienten durch Anwendung derausgetauschten Informationen
  - die durch den Austausch von Informationen verbesserte Leistungsfähigkeit der verantwortlichen Organisation
- ✓ Daten- und Systemschutz
- ✓ Kompatibilität

Eine Unausgewogenheit zwischen diesen wesentlichen Merkmalen wird als

- Gefährdung für Patienten oder
- die Aufgabe der verantwortlichen Organisation gewertet.

3 Aufgaben und Verantwortlichkeiten

3.1 Allgemeines

Die Einbindung und Änderung von Geräten oder Software in ein MEDIZINISCHES IT-NETZWERK muss unter Rahmenbedingungen mit eindeutig festgelegten Verantwortlichkeiten erfolgen. Mindestens die Parteien, Verantwortlichkeiten und Anforderungen, die in den Unterabschnitten 3.2 bis einschließlich 3.6 benannt sind, müssen definiert werden.

Für das betrachtete medizinische IT-NETZWERK muss die VERANTWORTLICHE ORGANISATION eine

RISIKOMANAGEMENTAKTE für das MEDIZINISCHE IT-NETZWERK erstellen und pflegen.

3 Aufgaben und Verantwortlichkeiten

3.1 Allgemeines

Alle Unterlagen, die sich auf die Anforderungen dieser Norm an VERANTWORTLICHEN ORGANISATIONEN beziehen, sowie alle unterstützenden Unterlagen müssen in einer RISIKOMANAGEMENTAKTE für das MEDIZINISCHEIT-NETZWERK gepflegt werden. Diese Akte muss die aktuelle Information über das KONFIGURATIONSMANAGEMENT des medizinischen IT-NETZWERKS enthalten.

3.3 Verantwortung der OBERSTEN LEITUNG

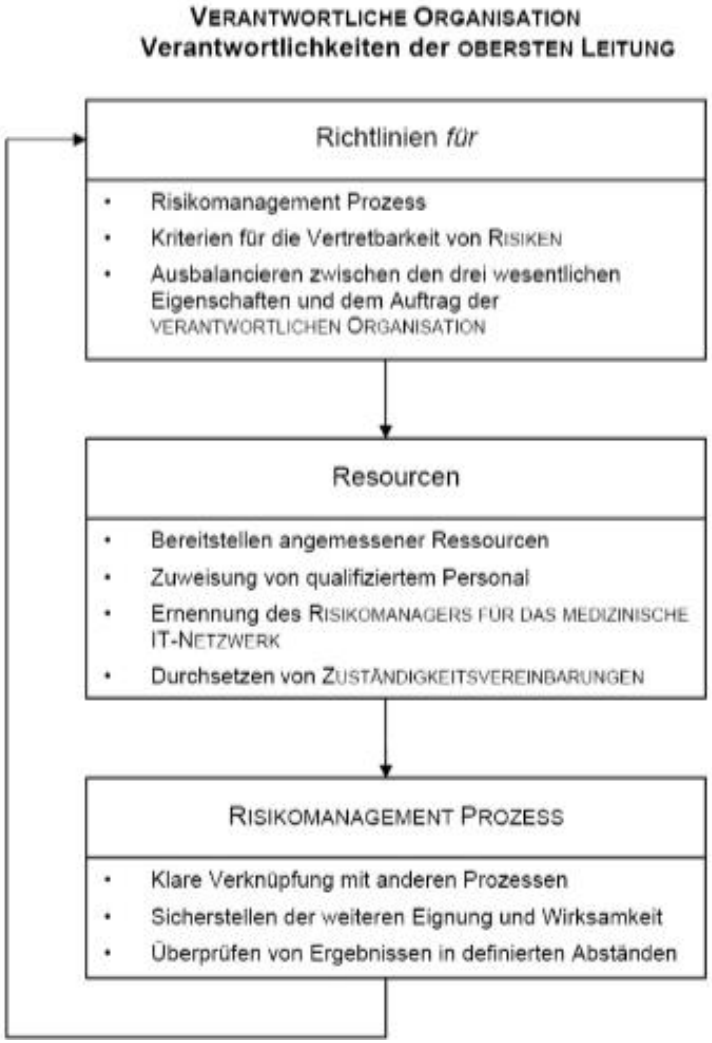
Für das Risikomanagement muss die oberste Leitung

- ✓ Eine Richtlinie für das Risikomanagement erstellen
- ✓ Eine Richtlinie definieren, wie vertretbare Risiken bestimmt werden
- ✓ Die notwendigen Ressourcen bereitstellen
- ✓ Qualifiziertes Personal bereitstellen
- ✓ Ergebnisse der Risikomanagement-Aktivitäten, Management von Vorkommnissen regelmäßig prüfen (PDCA)

Alle Punkte müssen in der Risikomanagementakte für das medizinische IT-Netzwerk dokumentiert werden.

- ✓ Sicherstellen der Zusammenarbeit mit dem Risikomanager
- ✓ Vollständigkeit des Risikomanagementprozesses ...

DIN EN 80001-1:2011-11



3.4 Risikomanager für das medizinische IT-Netzwerk

... ist für die Organisation und Durchführung des RM-Prozesses verantwortlich.

... überwacht die Durchführung des RM-Prozesses

... ist verantwortlich für die folgenden Aspekte:

a) Organisation und Durchführung des RM-Prozesses,

b) Berichte an die oberste Leitung über den RM-Prozess,

c) Sicherstellung der Kommunikation zwischen Teilnehmern wie

1) Hersteller von Medizinprodukten

2) andere Lieferanten von IT-Geräten, Software und Dienstl.

3) interne IT-Abteilung; andere Abteilungen des Gebäudemgmt

4) Anwender aus dem Gesundheitswesen

5) technische Abteilungen, (Betreuung der Medizinprodukte)

3.4 Risikomanager für das medizinische IT-Netzwerk

... ist verantwortlich für die Durchführung des RM-Prozesses:

d) Zusammenstellung aller Informationene) Planung der Einbindung der Medizinprodukte gemäß Herstellerang.

f) RM-Prozess, wenn ein Medizinprodukt hinzugefügt wird;

g) RM-Prozess, bei Ändrg. Medizinprodukt oder das med. IT-Netzwerk

h) Autorisierung für Inbetriebnahme nach Änderung;

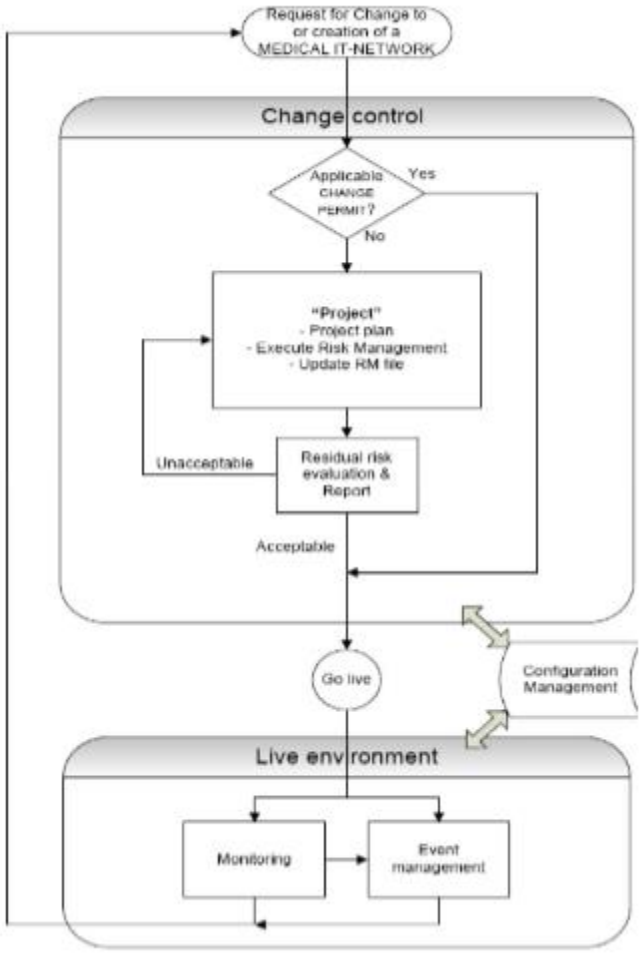
i) Information an die verantwortliche Organisation über unvertretbare Risiken und die möglichen Gefährdungen infolge von Änderungen;

j) Überwachung aller Projekte/Veränderungen am med. IT-Netzwerk, für die der Risikomanager verantwortlich ist.

Die Aufgaben können delegiert werden, aber der Risikomanager bleibt verantwortlich.

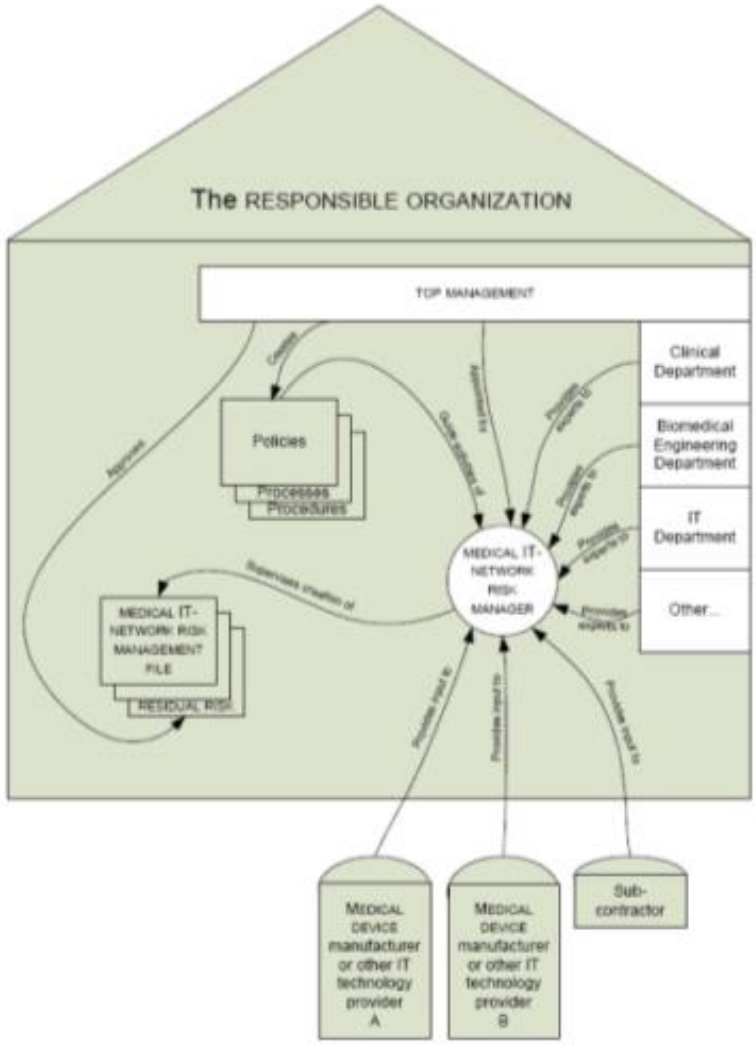
4 Risikomanagement für medizinische IT-Netzwerke

Übersicht über das Lebenszyklus-Risikomanagement für medizinische IT-Netzwerke



Info Anhang B

Übersicht über die Risikomanagement Verknüpfung



DIN ISO 27001:2013

- ✓ Informationstechnik –
- ✓ IT-Sicherheitsverfahren –Informationssicherheits-Managementsysteme – Anforderungen(ISO/IEC 27001:2013 + Cor. 1:2014)

0.1 Allgemeines

Diese Internationale Norm wurde erarbeitet, um Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines Informationssicherheitsmanagementsystems (ISMS)festzulegen. Die Einführung eines Informationssicherheitsmanagement-systems stellt für eine Organisation eine strategische Entscheidung dar. Erstellung und Umsetzung eines ISMS innerhalb einer Organisation richten sich nach deren Bedürfnissen und Zielen, den Sicherheits-anforderungen, den organisatorischen Abläufen sowie nach Größe und Struktur der Organisation.

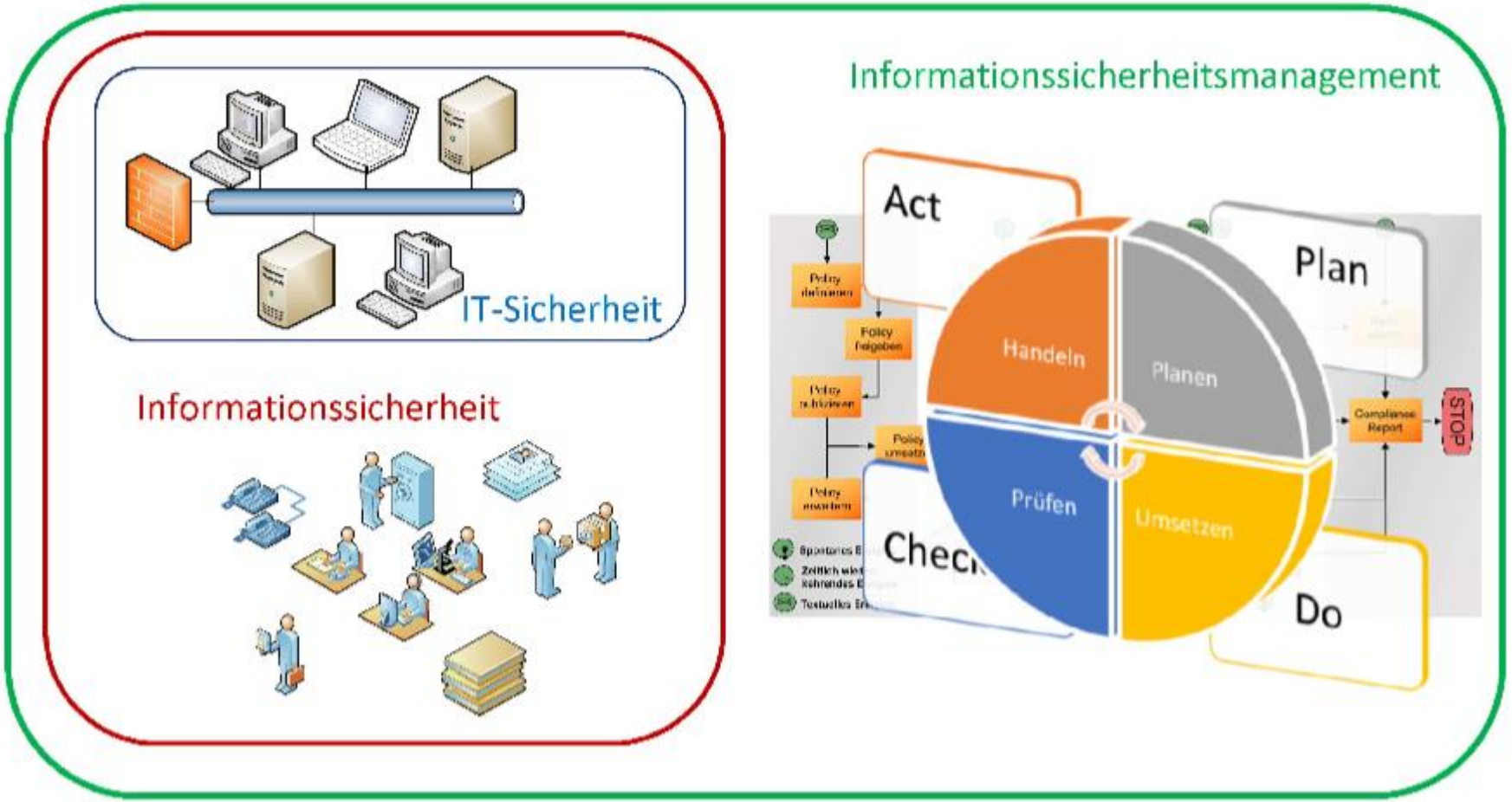
Das Informationssicherheitsmanagementsystem wahrt die Vertraulichkeit, Integrität und Verfügbarkeit von Information unter Anwendung eines Risikomanagementprozesses und verleiht interessierten Parteien das Vertrauen in eine angemessene Steuerung von Risiken.

0.2 Kompatibilität mit anderen Normen für Managementsysteme

Diese Internationale Norm wendet die Grundstrukturen, den einheitlichen Basistext, die gemeinsamen Benennungen und die Basisdefinitionen für den Gebrauch in Managementsystemnormen an, die jeweils im Anhang SL der ISO/IEC-Direktiven, Teil 1, „Consolidated ISO Supplement“ festgelegt sind, und stellt so die Übereinstimmung mit anderen Managementsystemnormen her, die ebenfalls den Anhang SL anwenden.

Organisation des ISMS

DIN ISO 27001:2013 Definition ISMS



Sicherheitsanforderungen

- ✓ Im Rahmen einer Risikobewertung werden die Bedrohungen für die Vermögenswerte identifiziert
- ✓ Schwachstellen und Wahrscheinlichkeit des Schadenseintritts bewertet und potentielle Auswirkungen abgeschätzt
- ✓ Das Unternehmen muss die gesetzlichen, sonstigen rechtlichen, behördlichen und vertraglichen Anforderungen erfüllen
- ✓ Eigene Grundsätze, Ziele und Geschäftsanforderungen an die Informationsverarbeitung sind zu beachten

Bewertung der Sicherheitsrisiken

- ✓ Die Sicherheitsanforderungen werden identifiziert. Der Aufwand für Maßnahmen wird dem wahrscheinlich entstehenden Schaden gegenübergestellt
- ✓ Die Ergebnisse der Risikobewertung helfen dabei, angemessene Handlungen und Prioritäten für die Risikobehandlung zu setzen und Maßnahmen zum Schutz gegen diese Risiken zu implementieren
- ✓ Die Risikobewertung wird in regelmäßigen Abständen wiederholt, um Änderungen Rechnung zu tragen

Ziel ist es Risiken zu verringern

Risikopunkte	AUSWIRKUNG				
Eintritts-wahrscheinlichkeit	Niedrig (1)	Mittel (2)	Hoch (3)	Sehr Hoch (4)	Immens (5)
Niedrig (1)	1	2	3	4	5
Mittel (2)	2	4	6	8	10
Hoch (3)	3	6	9	12	15
Sehr hoch (4)	4	8	12	16	20
Immens (5)	5	10	15	20	25

DIN ISO 27001:2013 Kontinuierl. Verbesserung

- ✓ Schulung der Mitarbeiter
- ✓ Prüfung auf Einhaltung der Prozesse und Maßnahmen (internes Audit)
- ✓ Überarbeitung und Verbesserung der Regeln(weniger ist manchmal mehr)
- ✓ Erstellung eines Notfallhandbuchs
- ✓ Einbeziehung weiterer Bereiche, z. B. externe Dienstleister, Lieferanten, Auftragsverarbeiter

DIN ISO 27001:2013 Hauptsicherheitskategorien

1. Sicherheitsleitlinien
2. Organisation der Informationssicherheit
3. Personalsicherheit
4. Management von organisationseigenen Werten
5. Zugriffskontrolle
6. Kryptographie
7. Schutz vor physischem Zugang und Umwelteinflüssen

DIN ISO 27001:2013 Hauptsicherheitskategorien

8. Betriebssicherheit
9. Sicherheit in der Kommunikation
10. Anschaffung, Entwicklung und Instandhaltung von Systemen
11. Lieferantenbeziehungen
12. Management von Informationssicherheitsvorfällen
13. Informationssicherheitsaspekte des Betriebskontinuitätsmanagements
14. Richtlinienkonformität

Die Maßnahmen des Anhang A der ISO 27001 werden in der ISO 27002 präzisiert.

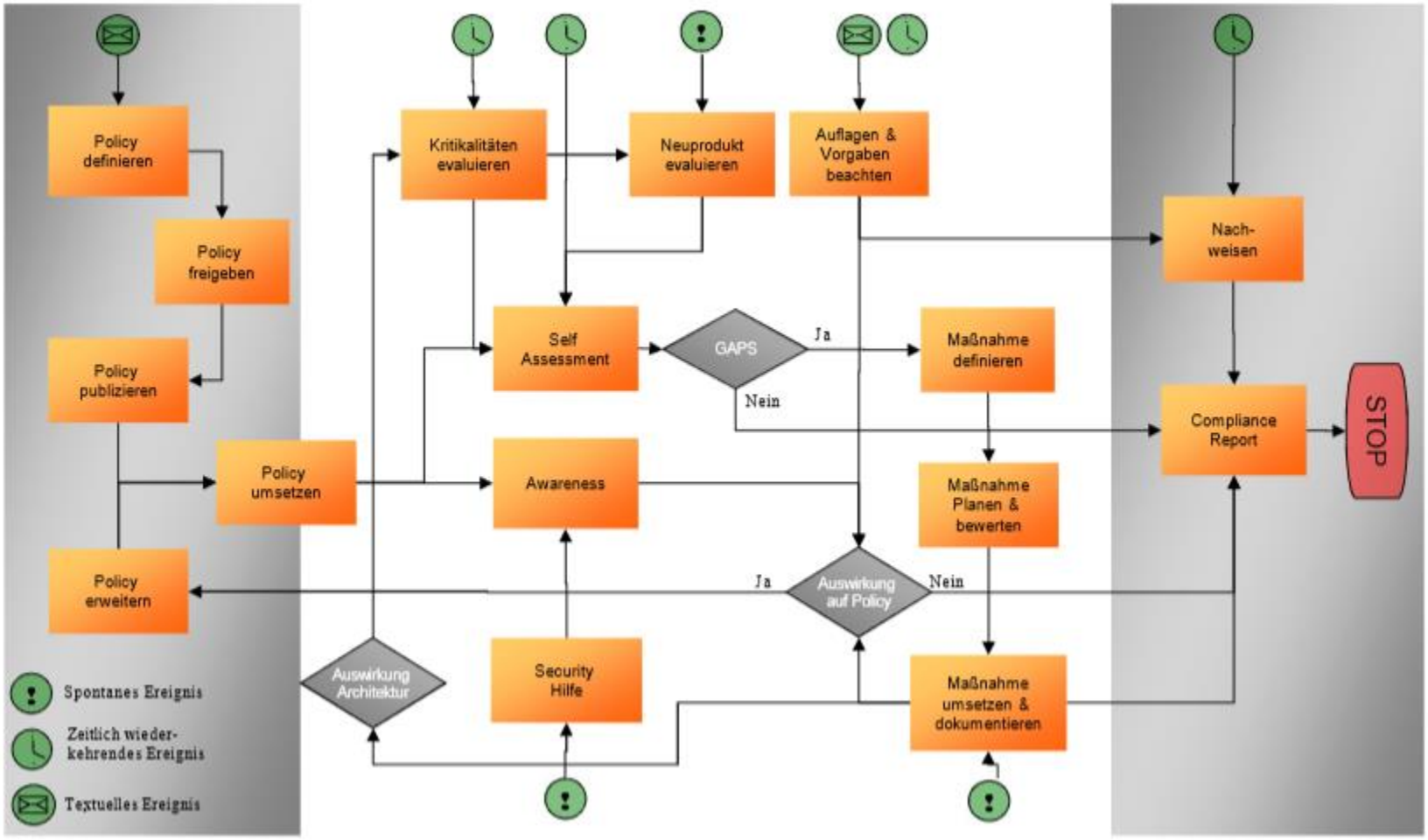
Das Managementsystem entspricht der Systematik der ISO 9000 (QM)Eine Zertifizierung ist nach ISO 27001 möglich.

DIN ISO 27001:2013 – BSiG-Referenzdoks

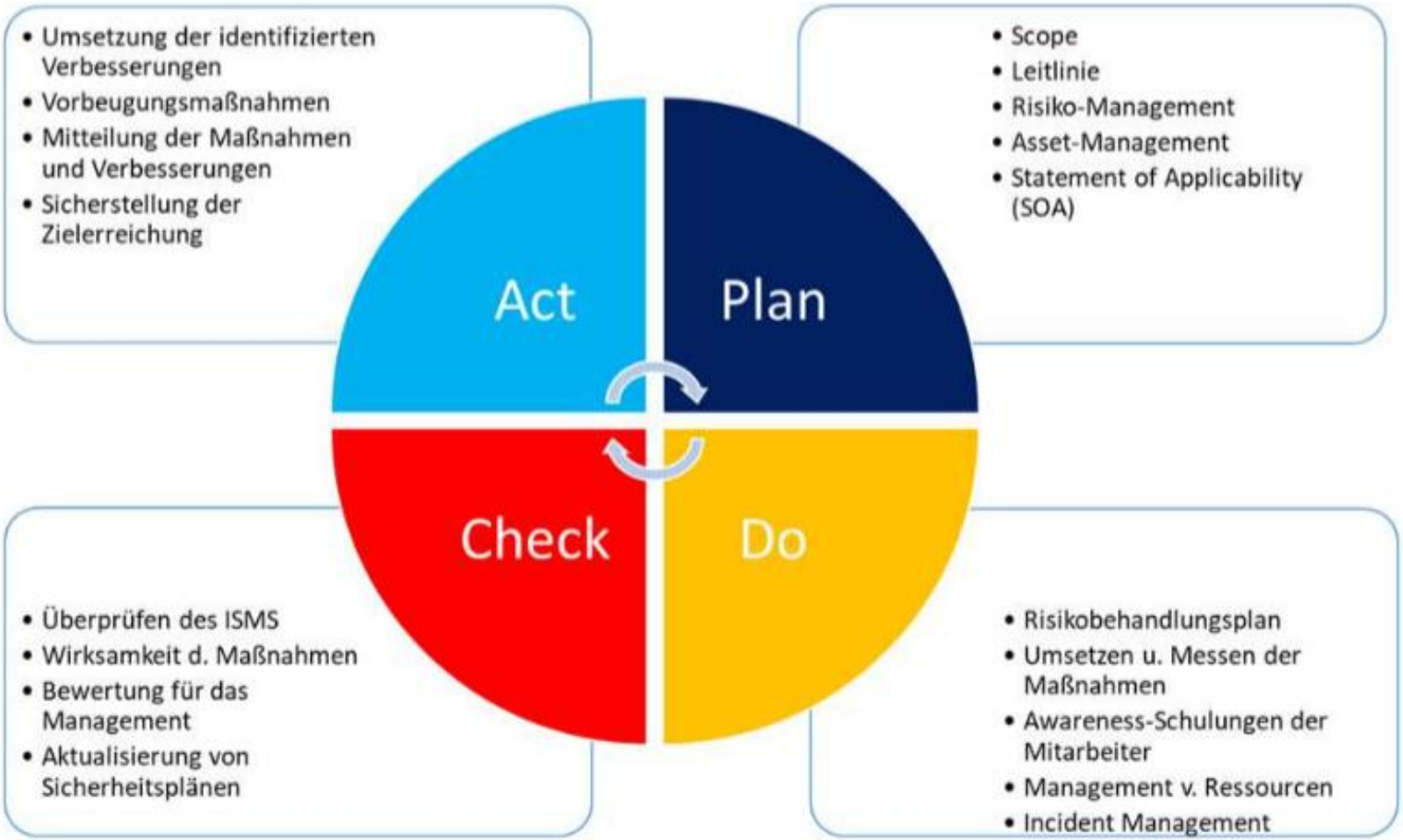
In Vorbereitung der Umsetzung eines ISMS wird die Erstellung der folgenden Leit- und Richtlinien empfohlen („A 0 Dokumente“ gemäß Liste der BSI-Referenzdokumente):

- ✓ Leitlinie zur Informationssicherheit
- ✓ Richtlinie zur Risikoanalyse
- ✓ Richtlinie zur Lenkung von Dokumenten und Aufzeichnungen
- ✓ Richtlinie zur internen ISMS-Auditierung
- ✓ Richtlinie zur Lenkung von Korrektur- und Vorbeugungsmaßnahmen

DIN ISO 27001:2013 ISMS als Prozess



DIN ISO 27001:2013 PDCA-Zyklus



ISO/IEC 20000-1

ISO/IEC 20000-1:2011-04 (E)

Information technology - Service management –

Part 1: Service management systemrequirements

- ✓ Kondensat von Good Practices
- ✓ Objectives und Controls
- ✓ Zertifizierung von Organisationen als Nachweis eines funktionierenden Management Systems möglich
- ✓ IT erhält Management Fokus
- ✓ QM erfährt Nutzen durch Fachwissen und Akzeptanz

ISO/IEC 20000-1

Die Norm erweitert ein vorhandenes ITIL V3 um

- ✓ Requirements for a management system (3)
- ✓ Planning and implementing Service Management (4)
- ✓ Planning and implementing new or changed services (5)

Das Managementsystem entspricht weitestgehend der Systematik der ISO 9000 Qualitätsmanagement

Die Norm ist Teil einer wachsenden Familie

- ✓ ISO/IEC 20000-2:2012-02 (E) Information technology - Service management –Part 2: Guidance on the application of service management systems
- ✓ ISO/IEC 20000-3:2012-08 (E) Information technology - Service management –Part 3: Guidance on scope definition
- ✓ ISO/IEC TR 20000-4:2010-12 (E) Information technology - Service management –Part 4: Process reference model and applicability of ISO/IEC 20000-1
- ✓ SO/IEC TR 20000-5:2013-11 (E) Information technology - Service management –Part 5: Exemplar implementation plan for ISO/IEC 20000-1
- ✓ ISO/IEC 20000-6:2017-06 (E) Information technology - Service management –Part 6: Requirements for bodies providing audit and certification of service management systems
- ✓ ...
- ✓ ISO/IEC TR 20000-10:2015-11 (E) Information technology - Service management –Part 10: Concepts and terminology
- ✓ ISO/IEC TR 20000-11:2015-12 (E) Information technology - Service management –Part 11: Guidance on the relationship between ISO/IEC 20000-1:2011 and service management frameworks: ITIL®
- ✓ ISO/IEC TR 20000-12:2016-10 (E) Information technology - Service management –Part 12: Guidance on the relationship between ISO/IEC 20000-1:2011 and service management frameworks: CMMI-SVC

BSI-Standard 100-4

Notfallmanagement

Version 2008 © BSI

1.2 Zielsetzung

Behörden und Unternehmen sind steigenden Risiken ausgesetzt, die die Produktivität oder die kontinuierliche und zeitnahe Erbringung ihrer Dienstleistungen für die Kunden gefährden. ...

Das Notfallmanagement ist ein Managementprozess mit dem Ziel, gravierende Risiken für eine Institution, die das Überleben gefährden, frühzeitig zu erkennen und Maßnahmen dagegen zu etablieren.

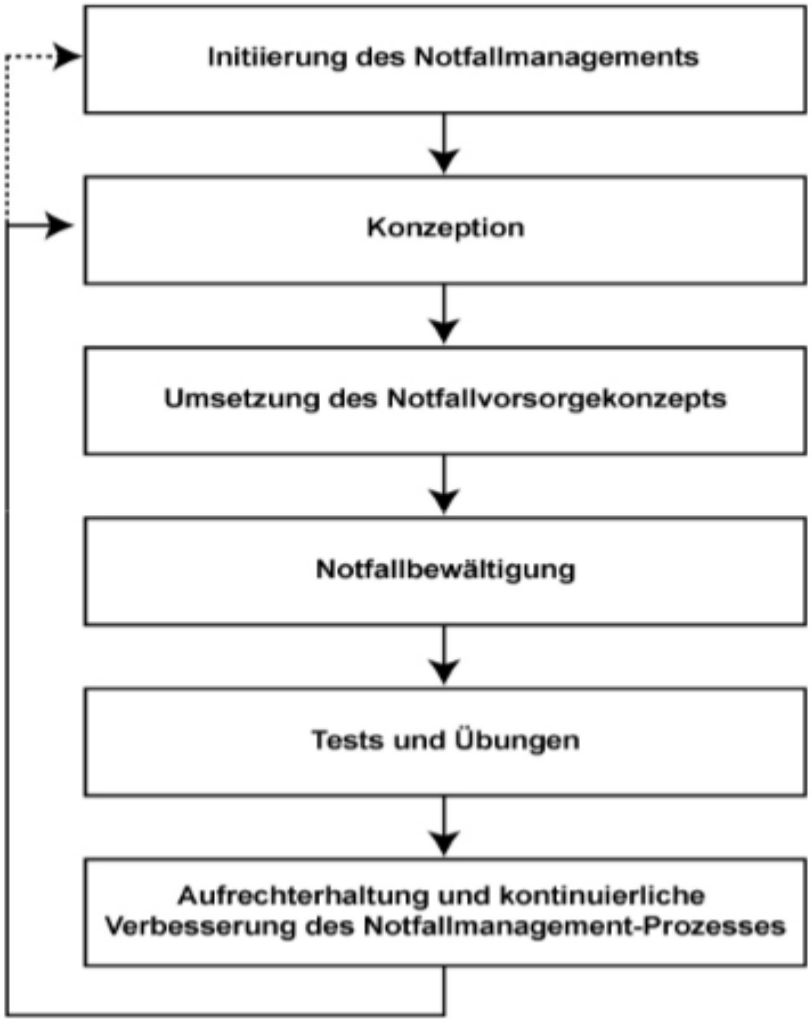
1.3 Adressatenkreis

Dieses Dokument richtet sich an Notfall- bzw. Business Continuity Manager, Krisenstabsmitglieder, Sicherheitsverantwortliche, -beauftragte, -experten und -berater, ...

BSI Standard 100-4

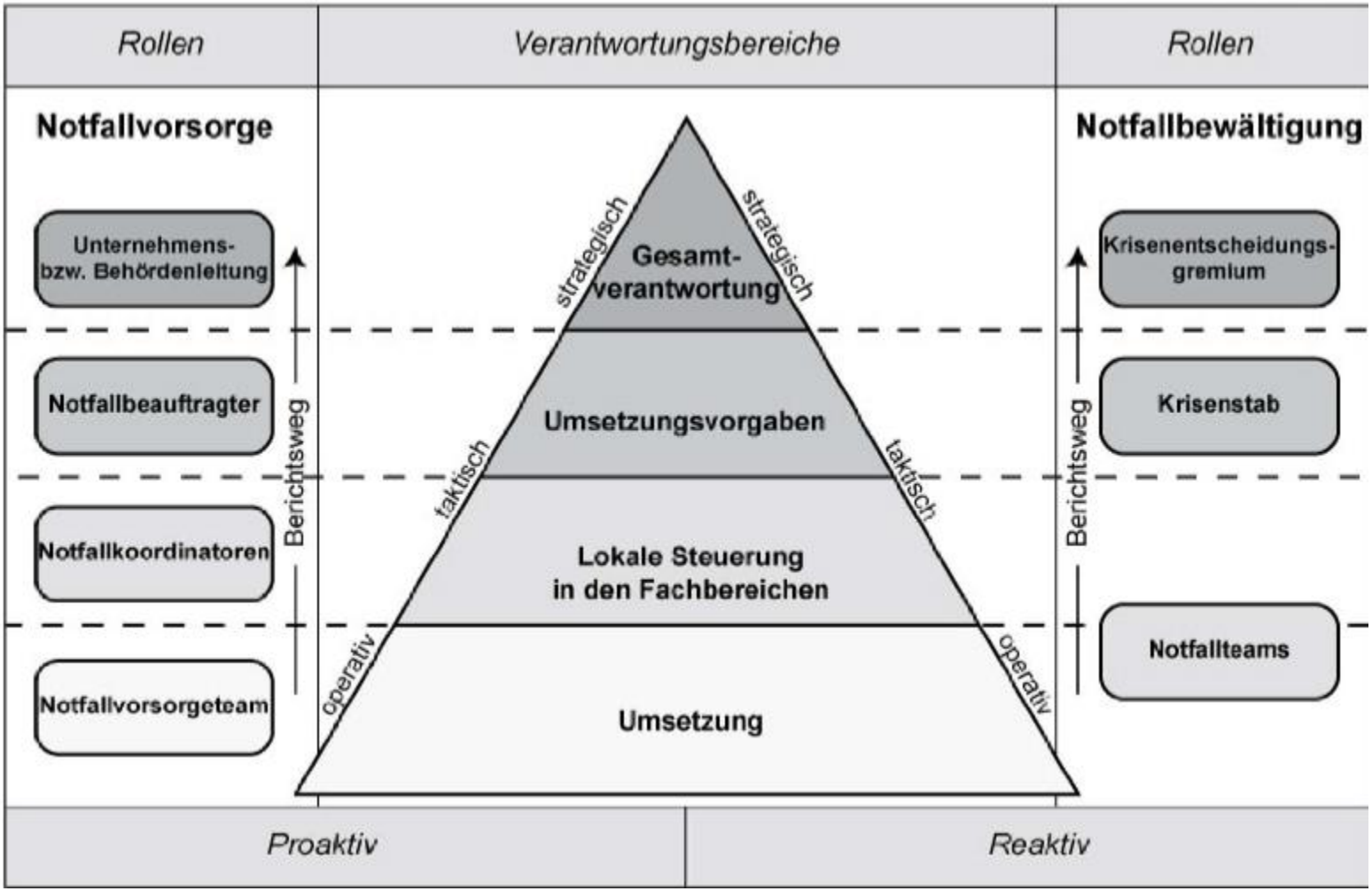
3.1 Überblick

Notfallmanagement-prozess



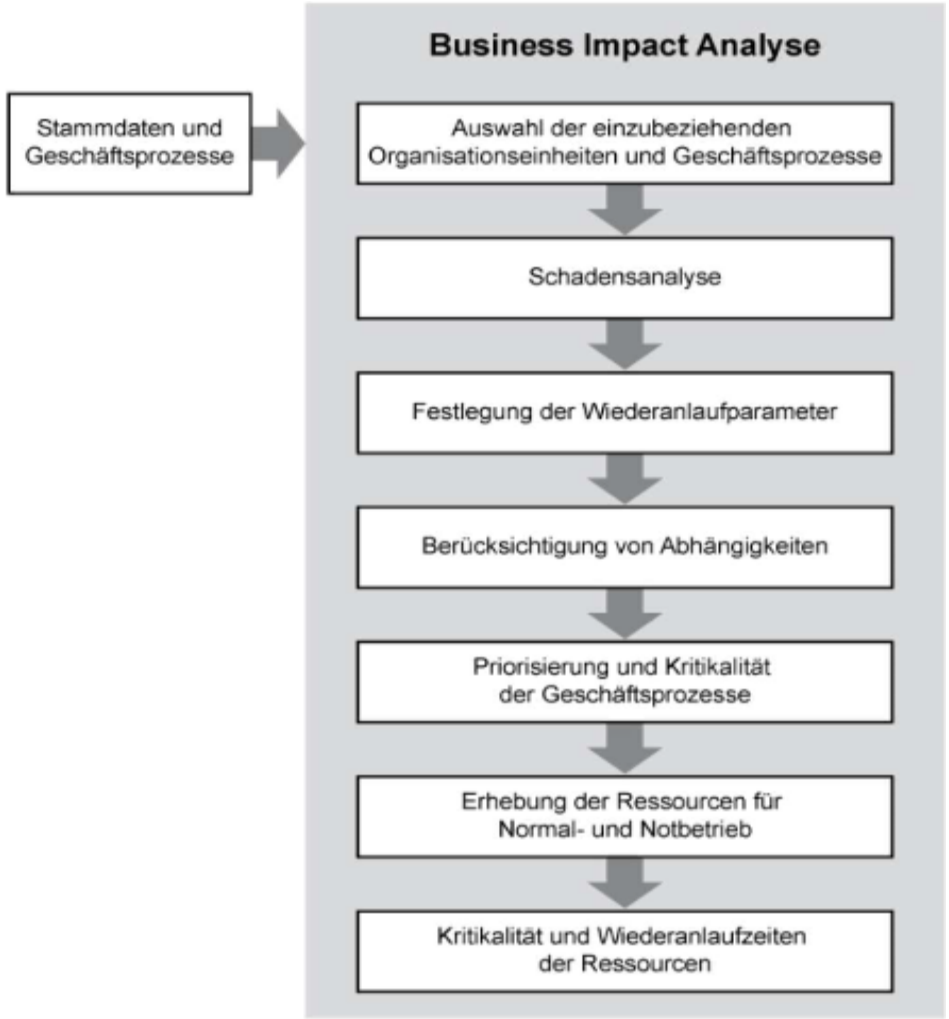
BSI Standard 100-4

4



BSI Standard 100-4

5.1.1 Business Impact Analysis



BSI Standard 100-4

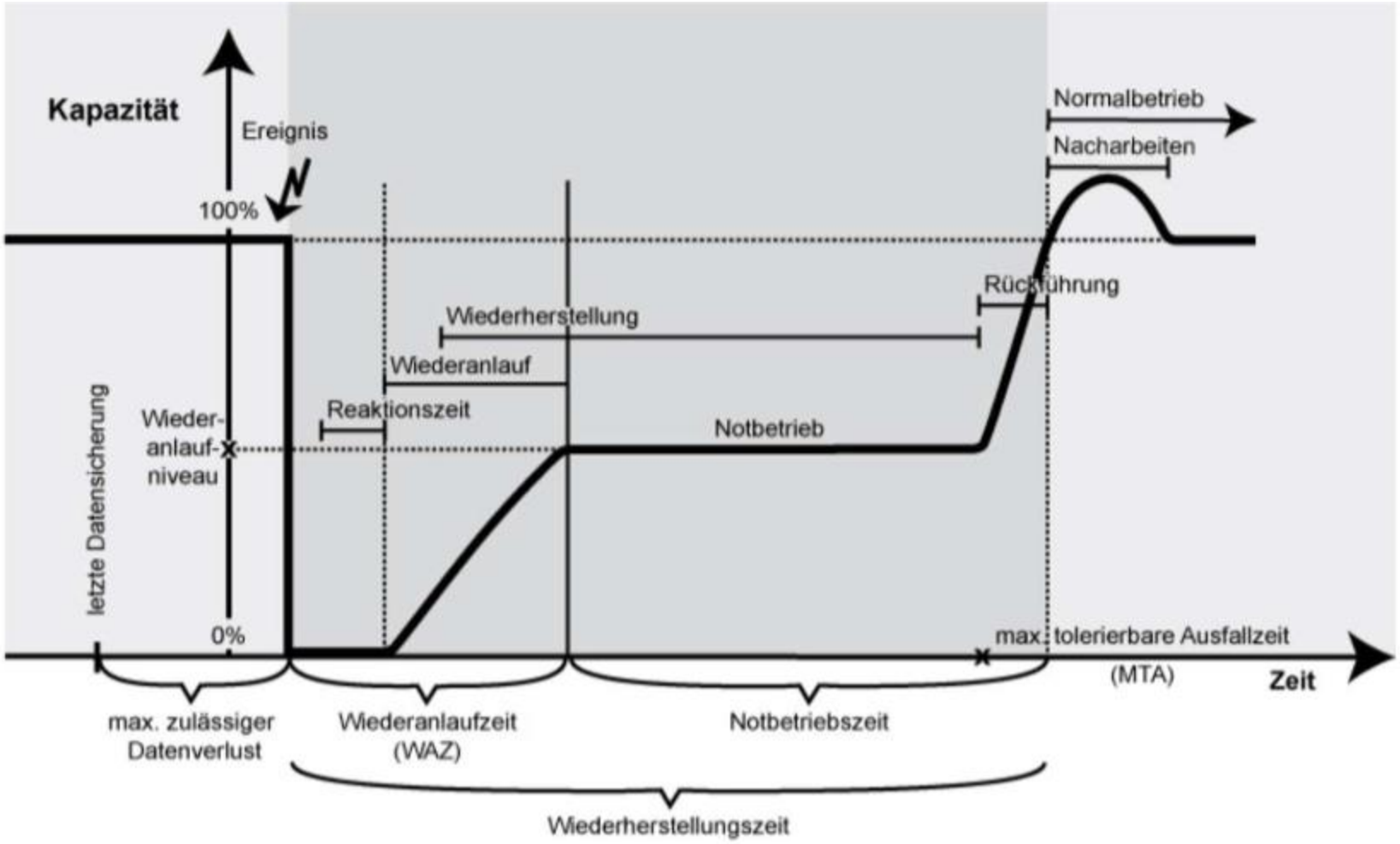
Hohe Komplexität

Prozess	Wiederanlauf	Wiederherstellung	Max. tol. Ausfall	24 Stunden	48 Stunden	96 Stunden	192 Stunden	Gewicht	Schadensszenario
P1				1	1	3			
				1	1	2			
				1	1	1	2		Imageschaden
				9	*9*	*22*	*31*		*Gew. Σ*
P2						3	4	5	finanzielle Auswirkungen
						3	3	3	Beeintr. der Aufgabenerfüllung
				1	1	2	3	1	Imageschaden
				9	*17*	*26*	*32*		*Gew. Σ*
P3				1	1	1	2	5	finanzielle Auswirkungen
				1	2	3	3	3	Beeintr. der Aufgabenerfüllung
				1	2	3	4	1	Imageschaden
				9	*13*	*17*	*23*		*Gew. Σ*
…	…		…	…	…	…	…	…	…
P12				1	1	2	4	5	finanzielle Auswirkungen
				1	2	3	3	3	Beeintr. der Aufgabenerfüllung
				1	1	1	1	1	Imageschaden
				9	*12*	*20*	*30*		*Gew. Σ*

Gewichteter Schaden nach 192 Stunden

Schadensanstieg

BSI Standard 100-4 Wiederanlaufparameter



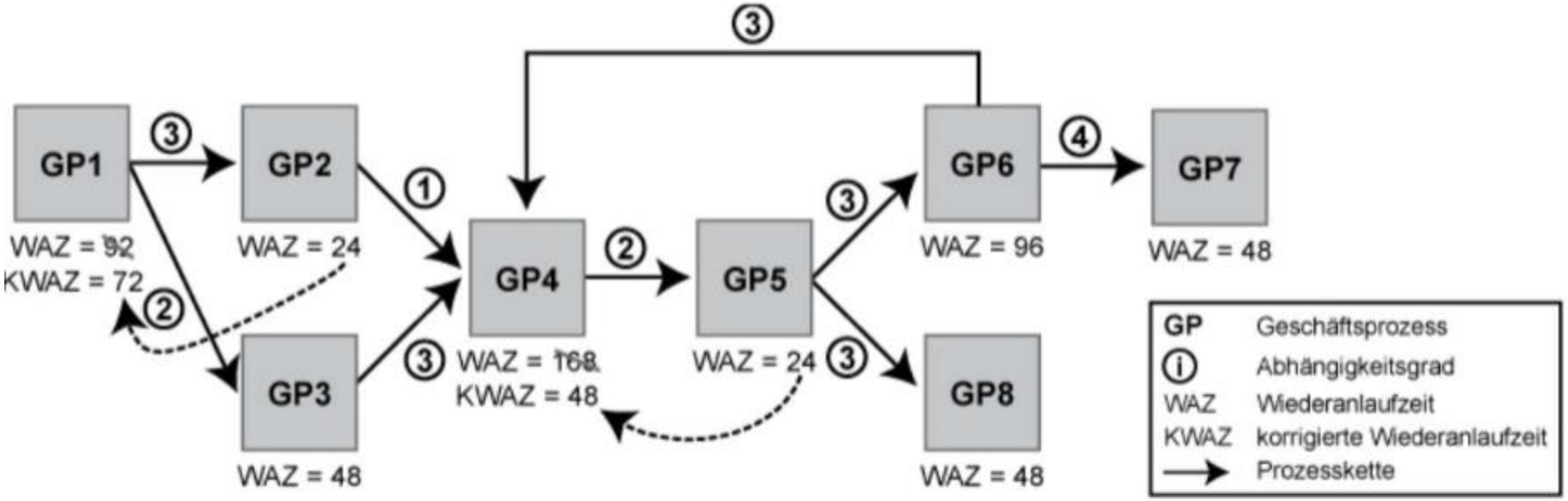


Abbildung 7: Vererbung der Wiederanlaufzeit in Richtung Vorgänger

5.2 Risikoanalyse

Die Risikoanalyse dient im Kontext des Notfallmanagements dazu, die Gefährdungen zu identifizieren, die eine Unterbrechung von Geschäftsprozessen verursachen können, und die damit verbundenen Risiken zu bewerten. Die Ziele sind,

- ✓ die bestehenden Risiken gegenüber den Entscheidungsträgern transparent zu machen,
- ✓ gegebenenfalls geeignete Strategien und Gegenmaßnahmen zu entwickeln, um diese Risiken im Vorfeld zu reduzieren und die Robustheit der Institution zu stärken, sowie
- ✓ die Szenarien zu identifizieren, für die individuelle Notfallpläne zu entwickeln sind.

BSI Standard 100-4

Fazit: Empfehlenswert

- ✓ Der BSI-Standard 100-4 eignet sich hervorragend für das Selbststudium
- ✓ Es werden konkrete Handlungsanleitungen gegeben und Umsetzungshilfen zum Download angeboten.
- ✓ An vielen Stellen wird zudem davor gewarnt, zu viele Risiken zu betrachten.
- ✓ Gleichzeitig blicken die Autoren weit über den Tellerrand hinaus und erklären anhand von Beispielen die Auswirkungen von Gefährdungen und unzureichender Notfallvorsorge.
- ✓ Viele Mechanismen und Beispieltabellen können im IT-Sicherheitsumfeld medizinischer IT-Netze verwendet werden.

Risk management — Principles and guidelines

1 Geltungsbereich

Dieser Internationale Standard enthält Grundsätze und allgemeine Richtlinien für das Risikomanagement.

Dieser Internationale Standard kann von jedem öffentlichen, privaten oder gemeinschaftlichen Unternehmen ... verwendet werden. Daher ist dieser Internationale Standard nicht branchenspezifisch.

Dieser Internationale Standard kann während der gesamten Lebensdauer einer Organisation und auf eine Vielzahl von Aktivitäten angewendet werden, ...

Dieser Internationale Standard kann auf jede Art von Risiko angewandt werden, unabhängig davon, ob es positive oder negative Auswirkungen hat.

ISO 31000

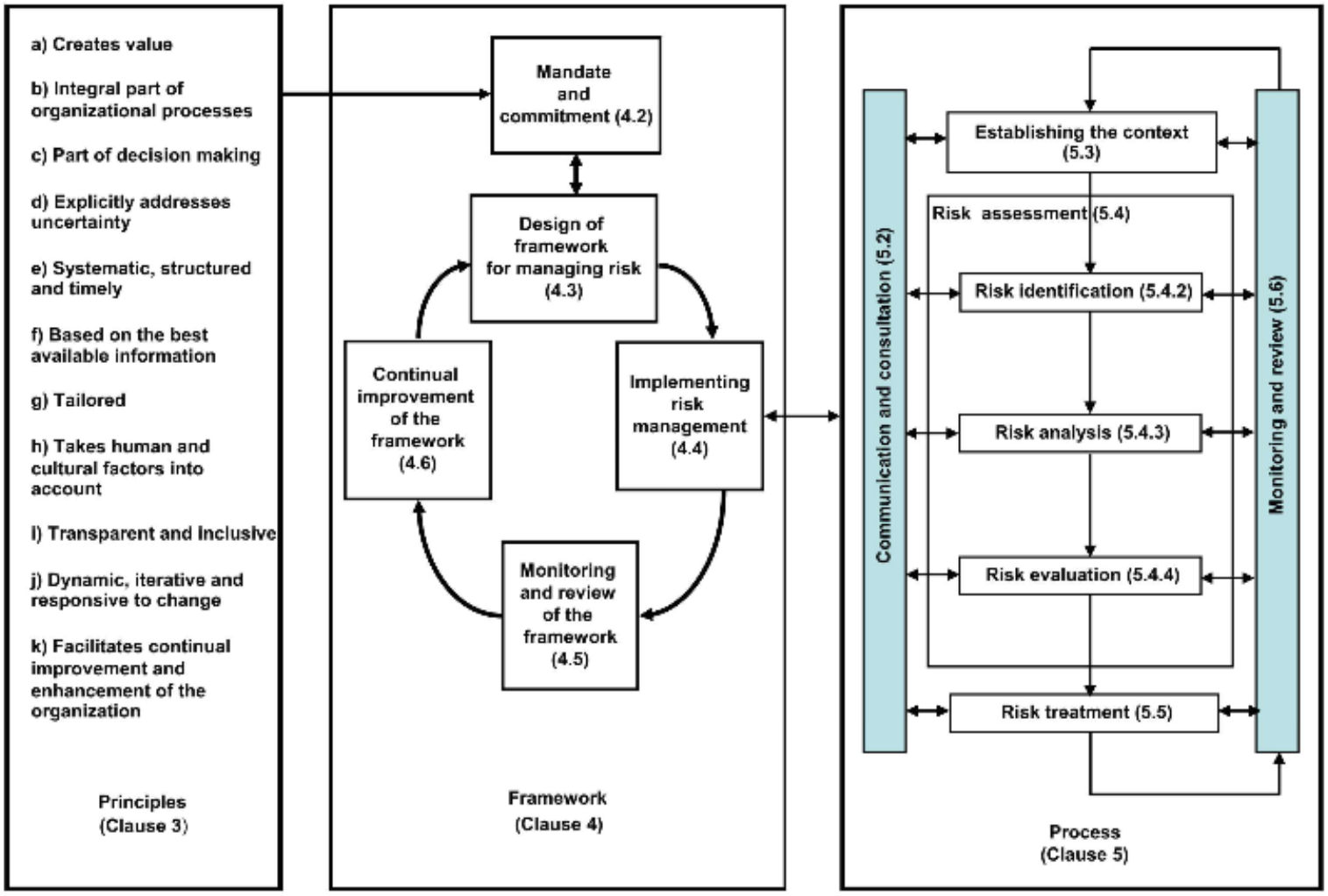


Figure 1 — Relationships between the risk management principles, framework and process

ISO 31000

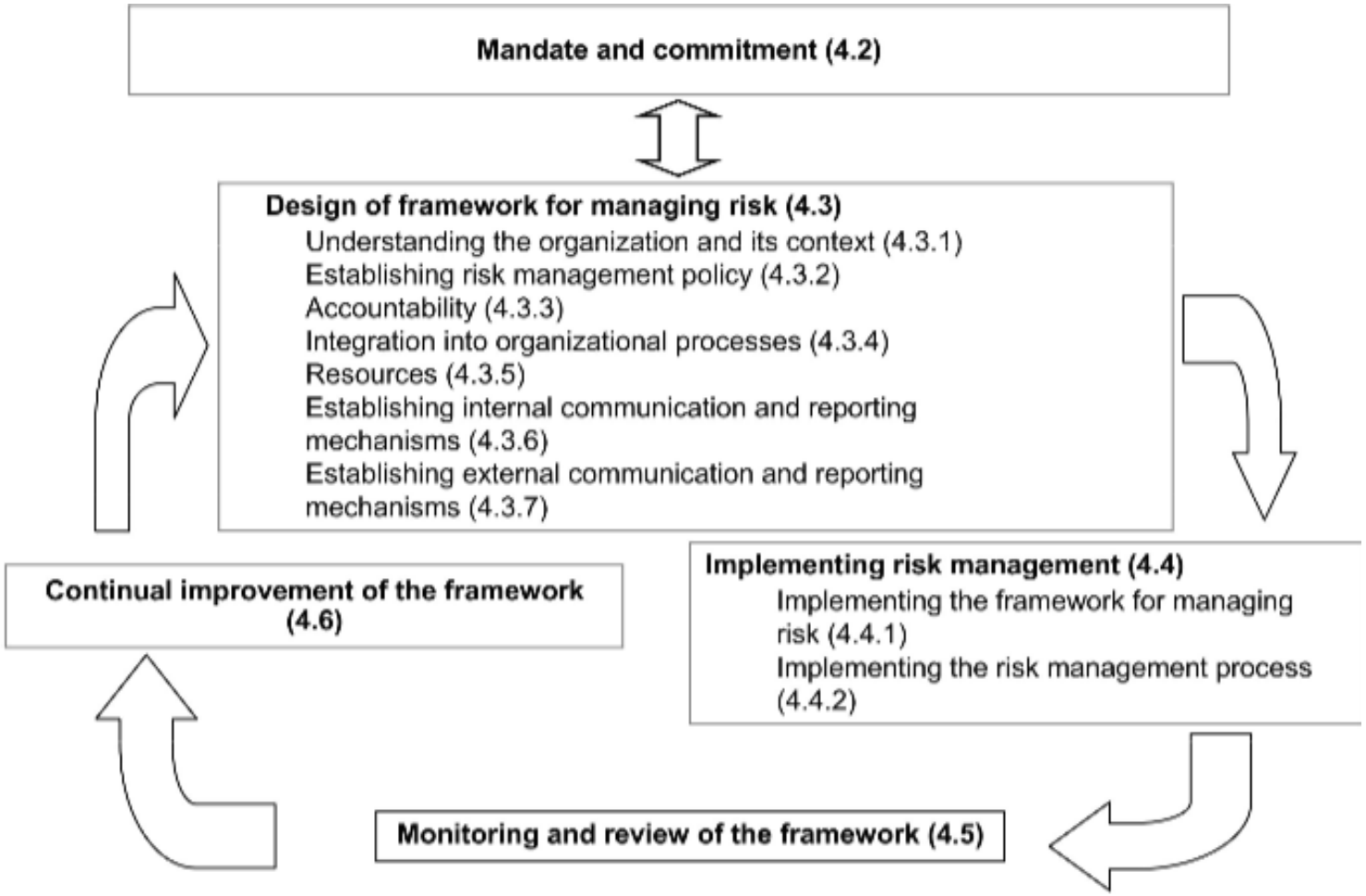


Figure 2 — Relationship between the components of the framework for managing risk

ISO 31000

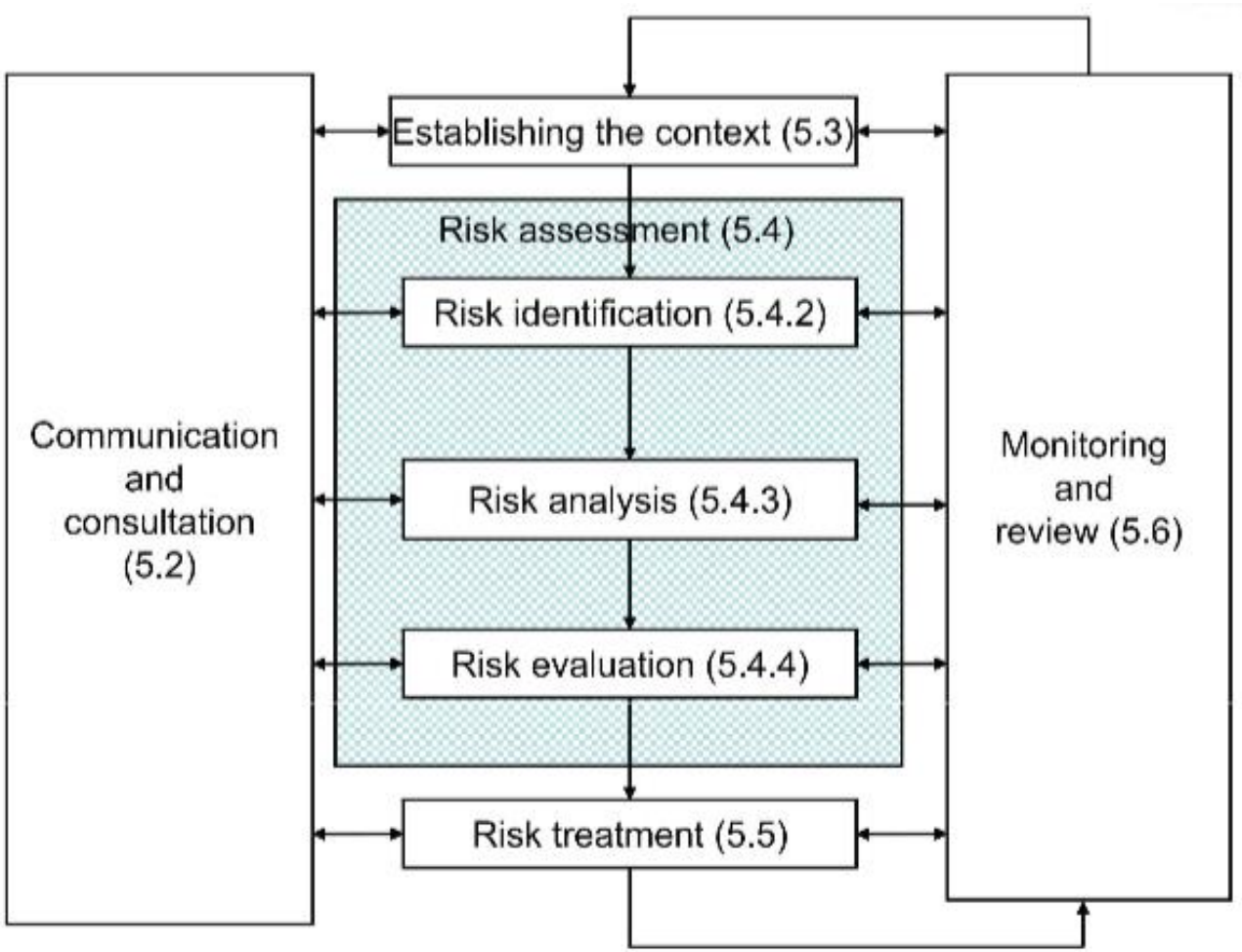


Figure 3 — Risk management process

DIN EN ISO 14971

Medical devices –
Application of risk management to medical devices
(ISO 14971:2007, Corrected version 2007-10-01)

Medizinprodukte –
Anwendung des Risikomanagements auf Medizinprodukte
(ISO 14971:2007, korrigierte Fassung 2007-10-01);

1 Geltungsbereich

Diese Internationale Norm legt einen Prozess fest, mit dem ein Hersteller die mit Medizinprodukten, einschließlich In-vitro-Diagnostika (IVD), verbundenen Risiken identifizieren, abschätzen und bewerten, diese Risiken kontrollieren und die Wirksamkeit der Kontrollen überwachen kann.

Die Anforderungen dieser Internationalen Norm gelten für alle Phasen des Lebenszyklus eines Medizinproduktes. Dieser Internationale Standard gilt nicht für die klinische Entscheidungsfindung. Diese internationale Norm legt keine akzeptablen Risikoniveaus fest. Diese Internationale Norm verlangt nicht, dass der Hersteller über ein Qualitätsmanagementsystem verfügt. Das Risikomanagement kann jedoch integraler Bestandteil eines Qualitätsmanagementsystems sein.

DIN EN ISO 14971

3 Allgemeine Anforderungen an das Risikomanagement

3.1 Risikomanagementprozess

Der Hersteller muss während des gesamten Lebenszyklus einen fortlaufenden Prozess zur Ermittlung der mit einem Medizinprodukt verbundenen Gefahren, zur Abschätzung und Bewertung der damit verbundenen Risiken, zur Kontrolle dieser Risiken und zur Überwachung der Wirksamkeit der Kontrollen einrichten, dokumentieren und aufrechterhalten. Dieser Prozess umfasst die folgenden Elemente

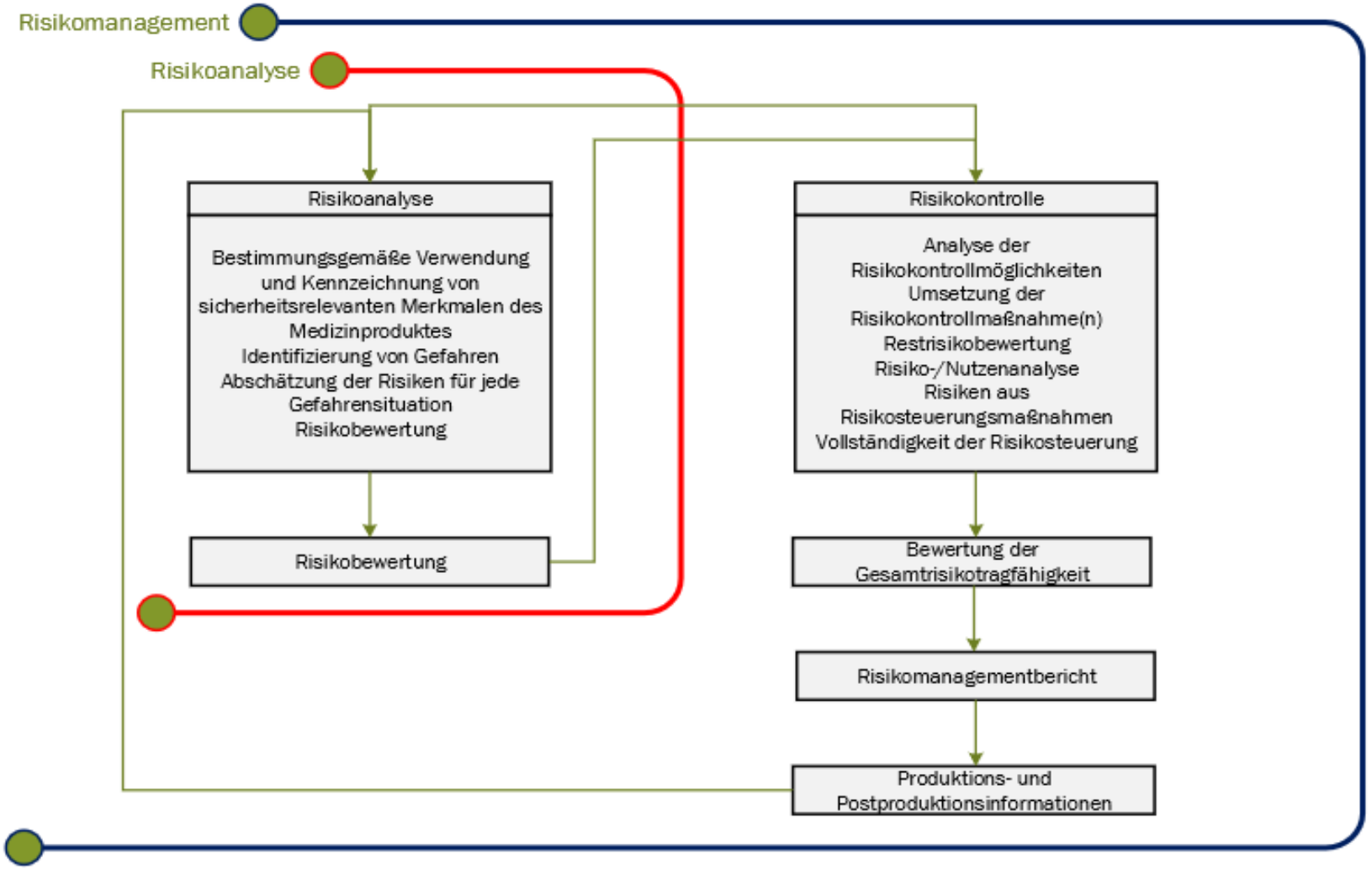
–Risikoanalyse;

–Risikobewertung;

–Risikokontrolle;

–Produktions- und Postproduktionsinformationen

DIN EN ISO 14971



DIN EN ISO 14971 risk management activities

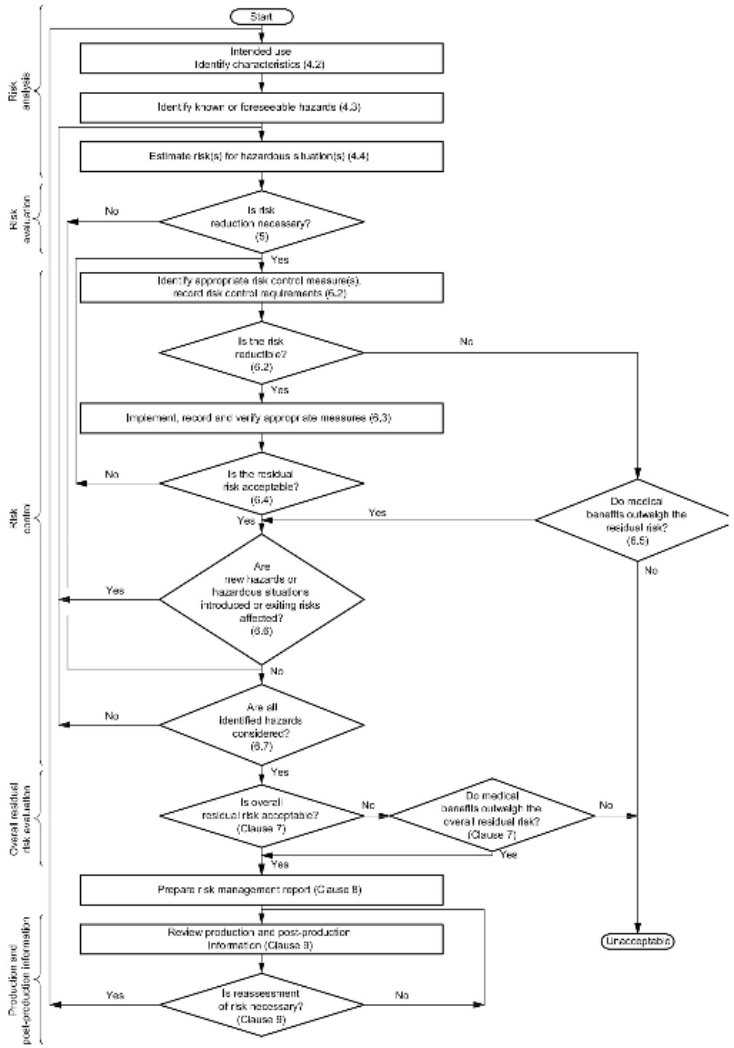


Figure B.1 — Overview of risk management activities as applied to medical devices

DIN EN ISO 14971

Tabelle A.1 – Zusammenhang zwischen ISO 14971 und IEC 80001-1			
	ISO 14971:2007 Abschnitt		IEC 80001-1 Abschnitt
4	RISIKOANALYSE		
4.1	RISIKOANALYSE PROZESS	n/a	
4.2	BESTIMMUNGSGEMÄßER GEBRAUCH und Identifizierung der Merkmale, die sich auf die SICHERHEIT beziehen		
4.3	Identifizierung von GEFÄHRDUNGEN	4.4.2	RISIKOANALYSE
4.4	Abschätzung der RISIKEN für jede Gefährdungssituation - „vernünftigerweise vorhersehbare Folgen oder Kombinationen von Ereignissen, die zu einer Gefährdungssituation führen können, müssen betrachtet werden und die daraus resultierenden Gefährdungssituationen müssen dokumentiert werden" - „Für jede identifizierte Gefährdungssituation müssen die dazugehörigen RISIKEN abgeschätzt werden		„Für jede identifizierte GEFÄHRDUNG muss die VERANTWORTLICHE ORGANISATION die dazugehörigen RISIKEN abschätzen…"
5	RISIKOBEWERTUNG	4.4.3	RISIKOBEWERTUNG
6	RISIKOBEHERRSCHUNG	4.4.4	RISIKOBEHERRSCHUNG
6.1	RISIKO-Verringerung	n/a	
6.2	Analyse der Optionen der RISIKOBEHERRSCHUNG	4.4.4.1	Analyse der Optionen der RISIKOBEHERRSCHUNG
6.3	Implementierung von Maßnahmen der RISIKOBEHERRSCHUNG	4.4.4.3	Implementierung von Maßnahmen der RISIKOBEHERRSCHUNG
		4.4.4.4	VERIFIZIERUNG der Maßnahmen der RISIKOBEHERRSCHUNG
6.4	Bewertung des RESTRISIKOS		(in 4.4.4.1 behandelt)
6.5	RISIKO/Nutzen-Analyse		(in 4.4.4.1 und 4.4.5 behandelt)
6.6	RISIKEN, die von Maßnahmen der RISIKOBEHERRSCHUNG herrühren	4.4.4.5	Neue RISIKEN, die aus der RISIKOBEHERRSCHUNG entstehen
7	Bewertung der Vertretbarkeit des Gesamt-RESTRISIKOS	4.4.5	Bewertung des RESTRISIKOS und Bericht

Ansprechpartner

CETUS Consulting GmbH
Frederik Humpert-Vrielink
Vriezenveenerstr. 38
48465 Schüttorf

Phone +49-(0)5923-90 35 67
Fax +49-(0)5923-90 37 85
frederik.humpert-vrielink@cetus-consulting.de