

Führung, Governance, Beschaffung und Recht

Leitfaden für Geschäftsleitungen, Klinikträger, Aufsichtsgremien und verantwortliche Fachbereiche

Die technischen und betrieblichen Risiken der übrigen Bände in klare Zuständigkeiten, dokumentierte Entscheidungen, belastbare Beschaffung und eine getrennt geprüfte Pflichtenlage übersetzen.

Fassung 1.0 · Stand 25. September 2026 · Adressaten: Geschäftsführung, Vorstand, Aufsichts- und Prüfungsgremien, ärztliche und technische Leitung, Informationssicherheit, Recht, Datenschutz, Personal, Einkauf und interne Revision.

Dokumenttyp: Fachliche Entscheidungsgrundlage; individuelle Rechtsprüfung und Organfreigabe erforderlich

Die Fallstudien in diesem Leitfaden-Paket sind ausdrücklich konstruierte Prüfbeispiele; eine externe wissenschaftliche, klinische, juristische oder sicherheitstechnische Begutachtung des Pakets hat nicht stattgefunden.

Steckbrief

Merkmal	Wert
Dokumenttyp	Fachliche Entscheidungsgrundlage; individuelle Rechtsprüfung und Organfreigabe erforderlich
Zielgruppe	Geschäftsführung, Vorstand, Aufsichts- und Prüfungsgremien, ärztliche und technische Leitung, Informationssicherheit, Recht, Datenschutz, Personal, Einkauf und interne Revision.
Recherche- und Rechtsstand	25. September 2026
Umfang	4.025 Wörter, 14 Seiten
Belege	0 Literatureinträge, 15 Quellenadressen
Gliederung	20 nummerierte Abschnitte, 2 Tabellen

Inhalt

1. Die Leitungsentscheidung betrifft Handlungsmacht	4
2. Zunächst die richtige Rolle bestimmen	4
3. Rechts- und Quellenstatus dieses Bandes	4
4. Pflichten- und Anwendungslandkarte	4
5. BSIG und Krankenhausrecht ohne pauschale Gleichsetzung	5
6. Aktuelle EU-Zeitachse: getrennte Fristen statt eines einzigen KI-Stichtags	5
7. Mehrere Meldepflichten können parallel entstehen	6
8. Datenschutz ist mehr als Vertraulichkeit	6
9. Beschäftigteninteressen und Überwachung	6
10. Verantwortungsmodell für normale Entscheidungen und Krisen	7
11. Braucht es ein neues Gremium?	7
12. Neue Aufgaben, mögliche Rollen und realistischer Personalbedarf	7
13. Beschaffung beginnt mit Wirkung und Ausfall	8
14. Vertrags- und Nachweisthemen	8
15. Budget und Priorisierung	8
16. Einführung in überprüfbaren Stufen	9
17. Berichte an Leitung und Aufsicht	9
18. Wissenschaftliche und fachliche Freigabe dieses Anhangs	9
19. Fragen, die ein Ausschuss stellen sollte	10
20. Arbeitsunterlagen und Ergebnis	10
Literatur und Quellenstatus	10
12 Rechtliche Hinweise	13
12.1 Keine Beratung	13
12.2 Keine Zusicherung, keine Konformitätsaussage	13
12.3 Rechtsstand	13
12.4 Haftung	13
12.5 Verweise auf fremde Inhalte	13
12.6 Marken und Produktbezeichnungen	13
12.7 Urheberrecht und Nutzung	13
12.8 Keine personenbezogenen Daten	14
12.9 Unabhängigkeit	14
12.10 Anwendbares Recht	14

Impressum und Verantwortlichkeit

Die folgenden Angaben sind wörtlich dem Impressum von fluxlane.eu entnommen, abgerufen am 24. September 2026. Sie wurden nicht ergänzt und nicht umformuliert.

Angabe	Inhalt
Angaben gemäß § 5 DDG	WebTrades GmbH Am Ölberg 2 55459 Grolsheim Deutschland
Vertreten durch	Geschäftsführerin: Laurice Bussmer
Kontakt	Telefon: 0170 890 78 00 E-Mail: info@fluxlane.eu
Registereintrag	Eintragung im Handelsregister Registergericht: Amtsgericht Mainz Registernummer: HRB 54479
Umsatzsteuer-ID	Umsatzsteuer-Identifikationsnummer gemäß § 27 a Umsatzsteuergesetz: DE461650292
Redaktionell verantwortlich	Verantwortlich für den Inhalt nach § 18 Abs. 2 MStV: Laurice Bussmer, Am Ölberg 2, 55459 Grolsheim
Verbraucherstreitbeilegung	Wir sind nicht bereit oder verpflichtet, an Streitbeilegungsverfahren vor einer Verbraucherschlichtungsstelle teilzunehmen.

Redaktioneller Hinweis des Herausgebers (wörtlich)

„fluxlane ist ein unabhängiges, redaktionelles Fachportal für Robotik, autonome physische Systeme und verkörperte KI. Der redaktionelle Geltungsbereich umfasst Industrie und Produktion, Logistik, Medizin, Pflege und Rehabilitation, Service und Haushalt sowie Forschung, Hersteller, Markt und Regulierung; künstliche Intelligenz gehört dazu, auch ohne physischen Körper. Die Inhalte dienen der allgemeinen Information und stellen keine Rechts-, Kauf- oder Anlageberatung dar. Angaben zu Preisen, Verfügbarkeit und Terminen erfolgen ohne Gewähr und können sich jederzeit ändern.“

Zitierweise

FluxLane (2026): *Führung, Governance, Beschaffung und Recht – Leitfaden für Geschäftsleitungen, Klinikträger, Aufsichtsgremien und verantwortliche Fachbereiche*. Fassung 1.0, Stand 25. September 2026. Herausgegeben von der WebTrades GmbH, Grolsheim, fluxlane.eu.

Herstellung dieses Dokuments

Das vorliegende PDF ist maschinell aus der Markdown-Fassung des Leitfaden-Pakets gesetzt. Inhaltlich ist dieser Satzvorgang keine neue Sachprüfung; die zugrunde liegende Recherche- und Quellenprüfung ist im Lieferpaket dokumentiert. Setzt wurde mit IBM Plex Sans und Sora.

Abbildungsnachweis

Dieses Dokument enthält keine Abbildungen.

1. Die Leitungsentscheidung betrifft Handlungsmacht

Mit der Einführung eines Agenten wird nicht nur Software beschafft. Die Organisation entscheidet, welche Informationen ein System erhält, welche Handlungen es ausführen kann, welche Abhängigkeiten daraus entstehen und wer bei Fehlverhalten eingreifen darf. Diese Entscheidung kann nicht vollständig an Modellanbieter, Systemintegrator oder SOC ausgelagert werden.

Die Geschäftsleitung muss nicht jeden technischen Parameter selbst bestimmen. Sie benötigt aber eine Entscheidungsstruktur, die relevante Risiken sichtbar macht und fachliche Zuständigkeiten verbindet. Eine Budgetfreigabe ohne klaren Funktionsumfang kann sonst faktisch eine unkontrollierte Übertragung von Handlungsmacht erlauben. Umgekehrt kann eine Sicherheitsabteilung die Organisation handlungsunfähig machen, wenn sie ohne betrieblichen Auftrag jede Automatisierung pauschal blockiert.

NIST CSF 2.0 bietet mit seiner Governance-Funktion eine strukturierende Grundlage. Das Framework schreibt nicht für jede Organisation dasselbe Organigramm oder eine bestimmte technische Lösung vor. Diese Arbeit leitet daraus ein überprüfbares Entscheidungsverfahren ab: Nutzungszweck, Risiko, Verantwortlichkeit, Nachweis, Ausnahme und Wiederprüfung werden gemeinsam dokumentiert. [Q04]

2. Zunächst die richtige Rolle bestimmen

Eine Organisation kann in demselben Projekt mehrere Rollen besitzen. Sie kann Betreiberin einer Anlage, Arbeitgeberin, Verantwortliche für personenbezogene Daten, Auftraggeberin eines Dienstleisters und Nutzerin eines KI-Systems sein. Bei eigener Entwicklung, wesentlichen Änderungen oder Weitergabe eines Produkts können weitere Rollen relevant werden. Die konkrete Einstufung muss am jeweiligen Rechtsrahmen erfolgen.

Die Rollenklärung wird nicht als einmalige Formalie behandelt. Wenn ein zunächst lesender Assistent später eigenständig Aufträge schreibt, erweitert sich zumindest die technische und organisatorische Verantwortung. Ob daraus zusätzlich eine andere rechtliche Rolle entsteht, ist gesondert zu prüfen. Dasselbe gilt für einen Integrator, der eine neue Gesamtlösung schafft, oder einen Betreiber, der eine sicherheitsrelevante Funktion verändert.

Für jeden Anwendungsfall wird ein Rollenblatt angelegt. Es enthält Organisation, System, Verwendungszweck, Datenverarbeitung, Produkt-/Betriebsbezug, externe Beteiligte und die begründete rechtliche Zuordnung. Ein Eintrag „Hersteller ist verantwortlich“ reicht nicht aus, weil er weder den Gegenstand noch die verbleibenden Pflichten des Betriebs benennt.

3. Rechts- und Quellenstatus dieses Bandes

Die nachfolgende Matrix unterscheidet **geltende Pflichten mit zu prüfendem Scope, gestufte Anwendungsdaten, amtliche Erläuterungen, nicht verbindliche technische Orientierung** und **noch zu beschaffende Normvolltexte**. Der Unterschied ist materiell: Eine Empfehlung kann sinnvoll sein, ohne gesetzlich genau so vorgeschrieben zu sein. Ein Gesetz kann gelten, ohne ein bestimmtes Produkt oder eine bestimmte Organisationsform zu verlangen.

Die bereitgestellten deutschen Gesetzestexte zu BSIG, SGB V, BetrSichV und BetrVG konnten gelesen werden. Aktuelle Kommissionsseiten zum AI Act, zur Maschinenverordnung und zum CRA wurden ebenfalls gelesen. Mehrere direkte EUR-Lex-Volltextabrufe waren technisch blockiert. Wo diese Einschränkung besteht, wird nicht behauptet, der konsolidierte Normtext sei vollständig aktuell geprüft. Für konkrete Subsumtion, Vertragsgestaltung oder Freigabe ist dort die juristische Volltextprüfung ausdrücklich offen.

Diese Grenze ist kein Grund, die Arbeit auf allgemeine Warnungen zu beschränken. Die Matrix liefert die konkrete Suchstelle, die zu klärende Rolle, die relevante Entscheidung und den erwarteten Nachweis. Sie soll die individuelle Prüfung beschleunigen, nicht eine nicht durchgeführte Rechtsberatung vortäuschen.

4. Pflichten- und Anwendungslandkarte

Regelungsbereich	Zunächst zu klären	Fundstelle und gegenwärtige Grundlage
BSIG / NIS2-Umsetzung	Einrichtungsart, Größe, Sondertatbestände, kritische Anlage	Q29, § 28 und Anlagen; §§ 30–32, 38–39

Regelungsbereich	Zunächst zu klären	Fundstelle und gegenwärtige Grundlage
Krankenhaus-IT	Krankenhausbezug und Verhältnis zu KRITIS-Pflichten	Q30, § 391 SGB V, besonders Abs. 5
Arbeitsmittel / Betrieb	Arbeitgeber- und Betriebsbezug, konkrete Verwendung, Änderungen	Q31, § 3 BetrSichV
Datenschutz	Zwecke, Rechtsgrundlagen, Verantwortlichkeit, Auftragsverarbeitung, Betroffenenrisiken	Q38, Art. 5, 6, 9, 25, 28, 32–35, 38–39, 44 ff.; Volltextcheck offen
KI-Verordnung	Anbieter-/Betreiberrolle, Verwendungszweck, Hochrisikoeinstufung, Übergangsfall	Q33/Q34 aktuell gelesen; Q39 aktueller Normpfad
Maschinenproduktrecht	Produkt, Rolle, Inverkehrbringen, Integration, Änderung	Q35 aktuell gelesen; Q40 Normpfad
CRA	Produkt mit digitalen Elementen, Hersteller-/Stewardrolle, Ausnahmen	Q36/Q37 aktuell gelesen; Q41 Normpfad
Medizinprodukte	Zweckbestimmung, Produkt-/Systemrolle, sicherheitsrelevante Änderungen	Q22 als nicht bindende Cyber-Leitlinie; geltende MDR/IVDR und Betreiberregeln zusätzlich beschaffen
Beschäftigtenvertretung	Anwendbarkeit des Vertretungsrechts; technische Überwachung / Gesundheitsschutz	Q32, § 87 Abs. 1 Nr. 6 und 7; andere Trägerregime gesondert

Die Tabelle ist kein vollständiges Rechtskataster für jeden Sektor. Insbesondere länderrechtliche Klinik- und Katastrophenschutzvorgaben, branchenspezifische Spezialregeln, Verträge und Produktkonformität können weitere Anforderungen erzeugen. Ihre Prüfung wird im Rollenblatt als eigener Auftrag geführt. Eine leere Zeile bedeutet „nicht geprüft“, nicht „nicht anwendbar“.

5. BSIG und Krankenhausrecht ohne pauschale Gleichsetzung

Im BSIG sind Anwendungsprüfung, Risikomanagement, besondere Pflichten kritischer Anlagen, Meldung und Leitungsverantwortung getrennte Regelungsbereiche. § 38 adressiert Umsetzung, Überwachung und Schulung der Geschäftsleitungen besonders wichtiger und wichtiger Einrichtungen. Daraus folgt keine pauschale Aussage, dass jede Führungskraft jedes Unternehmens identische Pflichten nach dieser Vorschrift besitzt. [Q29, §§ 28 und 38]

§ 391 SGB V verhindert zugleich die fehlerhafte Schlussfolgerung, ein Krankenhaus außerhalb einer bestimmten KRITIS-Konstellation habe keine krankenhausspezifischen IT-Sicherheitsanforderungen. Der Zusammenhang mit BSIG-Pflichten wird in Absatz 5 ausdrücklich behandelt. [Q30]

Praktisch benötigt die Leitung eine schriftliche Einstufung mit zugrunde gelegten Fakten, Rechtsstand, Bearbeiter und Wiederprüfauslöser. Unternehmenswachstum, neue Leistungen, Umstrukturierung oder eine veränderte kritische Funktion können eine Überprüfung erforderlich machen. Ein unkommentiertes Online-Selbstauskunftsergebnis ist kein vollständiger Nachweis der tatsächlichen Einstufung.

6. Aktuelle EU-Zeitachse: getrennte Fristen statt eines einzigen KI-Stichtags

Die am Stichtag gelesene Kommissionsdarstellung berücksichtigt die 2026 geänderte AI-Act-Zeitachse. Sie nennt den **2. Dezember 2027** für Hochrisikoregeln bestimmter Anhang-III-Anwendungen und den **2. August 2028** für Hochrisiko-KI in regulierten Produkten. Zugleich bestehen andere bereits geltende Anwendungsteile. Der Anhang übernimmt daher nicht unesehen ältere allgemeine Hochrisiko-Daten aus dem Ausgangsmaster. [Q33, Application timeline; Q34]

Diese Daten sind keine pauschale Betriebserlaubnis bis zu einem zukünftigen Termin. Bestehende Produkt-, Datenschutz-, Arbeits- und Sicherheitsanforderungen bleiben nach ihrem eigenen Scope zu prüfen. Welche Hochrisikokategorie eine konkrete Anwendung betrifft und wie Übergangs-/Bestandsregeln wirken, muss anhand der konsolidierten Fassung beurteilt werden. Die aktuelle Kommissionsübersicht ist eine tragfähige Orientierung, ersetzt aber nicht diese Subsumtion. [Q39, offener Volltextcheck]

Die Maschinenverordnung gilt nach der Kommissionsübersicht grundsätzlich ab **20. Januar 2027**. Beim CRA liegt der allgemeine Anwendungsbeginn bei **11. Dezember 2027**, während bestimmte Hersteller-Meldepflichten bereits seit **11. September 2026** gelten. Auch hier unterscheiden sich Produkt, Rolle und konkrete Pflicht. [Q35; Q36; Q37]

7. Mehrere Meldepflichten können parallel entstehen

Ein Sicherheitsereignis kann eine Betriebsstörung, eine Verletzung personenbezogener Daten und einen produktbezogenen Cybervorfall zugleich darstellen. Die Organisation muss diese Prüfpfade getrennt führen. Eine Meldung an einen Hersteller ersetzt nicht automatisch eine Meldung an eine Behörde. Ein Behördenbericht erledigt nicht notwendigerweise die Information betroffener Personen oder vertragliche Informationspflichten.

Für den einschlägigen BSIG-Fall nennt § 32 eine frühe Erstmeldung innerhalb von höchstens **24 Stunden** und eine weitergehende Meldung innerhalb von höchstens **72 Stunden** nach Kenntnis eines erheblichen Sicherheitsvorfalls; die Vorschrift enthält weitere Status- und Abschlussregeln. Die Anwendbarkeit, Erheblichkeit und der konkrete Meldeweg sind mitzuerfassen. [Q29, § 32]

Die Kommission beschreibt für einschlägige CRA-Herstellerberichte ebenfalls 24-/72-Stunden-Stufen, aber unterschiedliche Abschlussbezüge: bei aktiv ausgenutzten Schwachstellen grundsätzlich spätestens 14 Tage nach Verfügbarkeit einer Korrekturmaßnahme, bei schwerwiegenden Vorfällen grundsätzlich innerhalb eines Monats ab der 72-Stunden-Meldung. Für Open-Source-Stewards nennt sie einen anderen Beginn ihrer Berichtspflichten. Die Gleichheit einzelner Zahlen macht die Verfahren nicht identisch. [Q37, What are the main rules?]

Für Datenschutzverletzungen sind die bekannten Anforderungen aus Art. 33 und 34 DSGVO gesondert am geltenden Text zu prüfen: Meldung an die Aufsicht ohne unangemessene Verzögerung und nach Möglichkeit binnen 72 Stunden, soweit der gesetzliche Risikomaßstab erfüllt ist; Information Betroffener bei dem dafür vorgesehenen höheren Risiko, vorbehaltlich der gesetzlichen Ausnahmen. Diese Zusammenfassung ist in diesem Paket ausdrücklich mit dem offenen Volltextcheck verknüpft. [Q38, Art. 33–34]

Das Incident-Formular enthält deshalb je Verfahren Auslöser, Kenntniszeitpunkt, zuständige Bewertung, Meldepflichtentscheidung, Frist, Empfänger, übermittelte Fassung und Nachmeldung. Unvollständige Erkenntnis darf nicht mit fehlender Zuständigkeit verwechselt werden. Welche Angaben zunächst vorläufig gemeldet und später ergänzt werden müssen, wird anhand der jeweiligen Regel beurteilt.

8. Datenschutz ist mehr als Vertraulichkeit

Datenschutz schützt nicht nur vor unerlaubtem Kopieren. Er betrifft die Zulässigkeit und Gestaltung der Verarbeitung, den vorgesehenen Zweck, Datenumfang, Betroffenenrechte und die Risiken der Verarbeitung. Ein technisch sicherer Agent kann datenschutzrechtlich problematisch sein, wenn er mehr Informationen verarbeitet als für seinen Zweck notwendig oder Informationen für einen anderen Zweck weiterverwendet.

Vor der Einführung werden Verarbeitungsvorgang, Datenquellen, Empfänger, Speicherorte, Aufbewahrung und Löschung dokumentiert. Bei Gesundheitsdaten und anderen sensiblen Informationen ist besondere Sorgfalt bei Rechtsgrundlage und Schutzmaßnahmen erforderlich. Ob eine Datenschutz-Folgenabschätzung notwendig ist, wird anhand des gesetzlichen Risikomaßstabs und der konkreten Verarbeitung geprüft, nicht allein anhand des Etiketts „KI“. Die relevanten Artikel sind im Quellenregister als juristische Prüfsuchstellen aufgeführt. [Q38]

Der Datenschutzbeauftragte braucht Zugang zu den notwendigen Informationen und die Möglichkeit unabhängiger Beratung. Er ist jedoch nicht der alleinige operative Incident Commander oder die Person, die unternehmerische Restrisiken akzeptiert. Eine Organisation darf ihre Verantwortung nicht dadurch verschieben, dass auf jeder Entscheidung „mit Datenschutz abgestimmt“ steht. Ebenso darf sie Datenschutzberatung nicht erst am Ende einer technisch bereits unumkehrbaren Einführung einholen.

9. Beschäftigteninteressen und Überwachung

Ein cyberphysisches SOC kann Geräte-, Prozess- und Nutzerereignisse zusammenführen. Dadurch können Informationen über Arbeitsleistung, Verhalten oder Anwesenheit entstehen, die über den Sicherheitszweck hinausgehen. Die Einführung braucht daher eine klare Zweckbegrenzung, Rollen für den Zugriff, Auswertungsregeln und angemessene Aufbewahrungsfristen.

Wo das Betriebsverfassungsgesetz anwendbar ist, sind die Mitbestimmungstatbestände insbesondere bei technischer Überwachung und Gesundheitsschutz zu prüfen. Für öffentliche oder kirchliche Träger können andere

Vertretungsregime gelten. Die Rechtsprüfung darf diese Unterschiede nicht durch ein pauschales Standardformular verdecken. [Q32]

Auch aus organisatorischer Sicht ist es problematisch, Sicherheitsprotokolle ohne transparente Regeln zur individuellen Leistungskontrolle zu verwenden. Beschäftigte können Unsicherheiten dann seltener melden oder Schutzmaßnahmen umgehen. Dies ist eine plausible Organisationshypothese, keine in diesem Paket gemessene Effektgröße. Daraus wird empfohlen, Meldesicherheit, Lernorientierung und die Trennung von Sicherheitsuntersuchung und anderen Personalzwecken ausdrücklich zu gestalten.

10. Verantwortungsmodell für normale Entscheidungen und Krisen

Eine sinnvolle Zuständigkeitsmatrix unterscheidet **entscheidungsverantwortlich**, **ausführungsverantwortlich**, **fachlich beteiligt** und **zu informieren**. Für jeden Entscheidungstyp wird genau eine koordinierende Entscheidungsstelle benannt; notwendige fachliche Mitfreigaben können daneben bestehen. Ein Feld mit fünf gleichberechtigten Gesamtverantwortlichen verhindert die Klärung eher, als dass es sie verbessert.

Entscheidung	Koordinierende Verantwortung	Unverzichtbare fachliche Beteiligung
Umfang autonomer Funktionen freigeben	Leitung des Leistungs-/Systembereichs innerhalb des Organmandats	Security, fachlicher Betrieb, bei Bedarf Safety/Medizintechnik und Datenschutz
Kritische Rechte ändern	benannter System-/Prozesseigentümer	IAM/Plattform, fachlicher Verantwortlicher, Sicherheitsprüfung
Vorfall technisch eingrenzen	Incident Commander im genehmigten Mandat	Betrieb und bei möglicher Gefährdung klinische/Safety-Verantwortung
Klinischen Ersatzmodus festlegen	zuständige klinische Leitung	Pflege, IT, Medizintechnik und betroffene Funktionsbereiche
Industriellen Wiederanlauf freigeben	zuständige Betriebsleitung	Schutzfunktionsprüfung, OT, Qualität und Instandhaltung
Gesetzliche Meldung veranlassen	verantwortliche Organisation über benannte Meldestelle	Recht, Security, gegebenenfalls Datenschutz/Produktsicherheit
Restrisiko akzeptieren	hierzu befugte Leitung	unabhängige Fachbewertung und dokumentierte Bedingungen

Die Matrix ersetzt keine gesetzliche Kompetenzordnung. Sie operationalisiert, wer innerhalb der Organisation eine Entscheidung vorbereitet und verantwortet. Notfallbefugnisse müssen so gestaltet sein, dass notwendige Schutzmaßnahmen nicht an einer unerreichbaren Einzelperson scheitern. Zugleich bleiben Reichweite, Dokumentation und nachträgliche Prüfung begrenzt.

11. Braucht es ein neues Gremium?

Ein gemeinsames Forum für Cybersecurity, Betrieb, Safety und KI kann sinnvoll sein, wenn diese Verantwortlichkeiten bisher getrennt entscheiden. Daraus folgt jedoch keine allgemeine gesetzliche Pflicht zu einem Organ namens „Cyber-Physical Resilience Board“. Der Begriff aus dem Master ist ein Organisationsvorschlag. Bestehende Risiko-, Sicherheits- oder Qualitätsgremien können die Aufgabe übernehmen, wenn Kompetenz, Mandat und Arbeitsweise ausreichen.

Das Forum bearbeitet wiederkehrende Grenzfragen: Welche Handlungsvollmacht ist zulässig? Welche Abhängigkeit ist akzeptabel? Welche Ausnahme läuft aus? Welche Nachweise fehlen vor einer Ausweitung? Welche Querschnittsrisiken betreffen mehrere Bereiche? Es ersetzt weder den Krisenstab noch die Fachprüfung. Seine Aufgabe ist die vorbereitende und nachverfolgende Entscheidung über Systemgrenzen und Risikoakzeptanz.

Ein Gremium ohne Beschlussfähigkeit, Ressourcen oder verbindliche Nachverfolgung erzeugt zusätzliche Sitzungen, aber keine nachweisbare Kontrolle. Deshalb gehören Mandat, Mitgliederrollen, Vertretung, Eskalation, Dokumentation und Entscheidungskompetenz in seine Geschäftsordnung. Die Sitzung endet mit konkreten Entscheidungen oder klar benannten offenen Punkten, nicht mit einem pauschalen Gesamtstatus.

12. Neue Aufgaben, mögliche Rollen und realistischer Personalbedarf

Die Aufgaben an den Schnittstellen können zusätzliche Qualifikationen oder Stellen rechtfertigen. Aus der vorliegenden Recherche lässt sich jedoch keine belastbare Zahl neuer Arbeitsplätze oder ein einheitlich etablierter neuer Beruf ableiten. Entscheidend ist zunächst, welche bislang unbesetzte Aufgabe tatsächlich erforderlich wird.

Ein **Cyber-Physical Security Engineer** kann beispielsweise Wirkungsketten zwischen IT und Anlage analysieren. Eine **Agent-Identity-Verantwortung** gestaltet Mandate und Delegation. Eine **klinische Cyberresilienz-Koordination** verbindet IT-Störung und Versorgung. Diese Bezeichnungen sind funktionale Vorschläge, keine neu geschaffenen geschützten Berufsabschlüsse. Bestehende Fachkräfte können Teile dieser Aufgaben übernehmen, sofern Kompetenz und Kapazität nachweisbar sind.

Der Personalbedarf wird aus Anlagen- und Anwendungsumfang, Änderungsfrequenz, Unterstützungszeiten, Nachweisaufwand und Vertretung abgeleitet. Eine einzige Spezialperson ohne Vertretung schafft eine neue kritische Abhängigkeit. Externe Unterstützung kann sinnvoll sein, wenn Rollen, Erreichbarkeit, Informationszugang und Grenzen vertraglich geregelt sind. Die Organisation behält dabei eine interne verantwortliche Stelle, die die externe Leistung beurteilen kann.

13. Beschaffung beginnt mit Wirkung und Ausfall

Ein Anforderungskatalog sollte nicht mit einer langen Funktionsliste beginnen, sondern mit dem vorgesehenen Nutzen und den nicht zulässigen Wirkungen. Welche Daten darf das System nutzen? Welche Aktionen darf es auslösen? Welche Funktionen müssen bei fehlender Verbindung erhalten bleiben? Welche Handlungen dürfen nie ohne zusätzliche Freigabe möglich sein? Daraus werden konkrete technische und vertragliche Nachweise abgeleitet.

Ein Anbieter soll die Antwort nicht allein im Vertriebsgespräch geben. Er liefert geeignete Dokumentation, Demonstration, Prüfberichte oder eine vereinbarte Abnahme. Beispielsweise wird ein eingeschränkter Betriebsmodus nicht nur beschrieben, sondern unter genehmigten Bedingungen vorgeführt. Ein Rollenmodell wird nicht nur als „granular“ beworben, sondern gegen konkrete unzulässige Aktionen geprüft.

Die Beschaffung bewertet auch die Möglichkeit der späteren Ablösung. Datenexport, Konfigurationsübernahme, Schlüssel- und Identitätsverwaltung sowie der Zugang zu notwendiger Betriebsdokumentation können für die Resilienz entscheidend sein. Ein Produkt, das nur mit dauerhaftem uneingeschränktem Herstellerzugang funktioniert, erzeugt eine andere Risikolage als ein Produkt mit begrenzten, widerrufbaren Servicezugängen. Die Entscheidung muss diesen Unterschied sichtbar machen.

14. Vertrags- und Nachweisthemen

Das Lieferantenformular bündelt fachliche Fragen zu Supportdauer, Sicherheitsupdates, Schwachstellenmeldung, Incident-Unterstützung, Unterauftragnehmern, Fernzugriff, Protokollen, Änderungen, Wiederherstellung und Datenrückgabe. Es enthält keine vorgeblich rechtssicheren Standardklauseln. Konkrete Vertragstexte müssen zum Produkt, Vergabeverfahren und zur Rechtsordnung passen.

Besonders wichtig sind widerspruchsfreie Zusagen. Ein Produkt darf nicht einerseits lokalen Betrieb versprechen und andererseits sämtliche Lizenzen über einen ständig erreichbaren zentralen Dienst erzwingen. Ein Datenlöschversprechen muss zu Protokollen, Sicherungskopien und notwendigen Nachweisen passen. Eine Updateusage muss erkennen lassen, wer Kompatibilität und Auswirkungen auf die konkrete Anwendung prüft.

Softwarestücklisten, Zertifikate und Auditberichte können wertvolle Nachweise sein. Sie müssen aber mit Scope, Version, Datum und Prüfstelle gelesen werden. Ein Zertifikat für ein Rechenzentrum ist kein Nachweis jeder Agentenberechtigung. Ein Bericht über die Entwicklungsorganisation ersetzt nicht die lokale Integrationsprüfung. Der Käufer benötigt daher ein Evidenzverzeichnis, das jede Anforderung mit dem tatsächlich passenden Nachweis verbindet.

15. Budget und Priorisierung

Eine angemessene Planung berücksichtigt Umsetzung und dauerhaften Betrieb. Neben Technik entstehen Kosten für Integration, Schulung, Vertretung, Protokollauswertung, Prüfungen, Übungen und die Pflege von Ersatzverfahren. Ein

Budget ohne diese Positionen kann formal eine sichere Architektur beschaffen und praktisch eine unbetreute Umgebung erzeugen.

Priorisiert werden zunächst dokumentierte kritische Pfade: unkontrollierte Vollzugriffe, unbekannte letzte Schutzfunktionen, fehlende Wiederherstellbarkeit oder nicht beherrschte Mindestversorgung. Komfortverbesserungen werden danach bewertet, ob sie diese Risiken tatsächlich reduzieren oder neue Abhängigkeiten erzeugen. Eine teure neue Plattform ist nicht automatisch wirksamer als eine gezielte Korrektur vorhandener Rechte und Verfahren.

Wirtschaftliche Abschätzungen benötigen offene Annahmen. Ausfallkosten, Wiederherstellungszeiten und Datenverluste dürfen nicht durch unbelegte Branchenmittelwerte präzise gerechnet werden. Wo Zahlen fehlen, werden Szenariobänder und Unsicherheiten dokumentiert. Gesetzlich notwendige oder fachlich unverzichtbare Schutzmaßnahmen werden nicht allein anhand einer hypothetischen Renditeentscheidung beurteilt.

16. Einführung in überprüfbaren Stufen

Eine lokale Einführung kann mit Bestandsaufnahme und der Sicherung offensichtlich unzulässiger Pfade beginnen. Danach werden ein begrenzter Pilot, die passende Kontrollarchitektur und ein geprüfter Ersatzprozess aufgebaut. Erst die Abnahme rechtfertigt die Erweiterung der Handlungsvollmacht. Die Stufen richten sich nach dem tatsächlichen Nachweisfortschritt, nicht nach einem künstlich einheitlichen Kalender.

Ein 30-/60-/90-Tage-Plan kann als Managementinstrument nützlich sein, darf aber keine unbewiesene Zusage suggerieren, in drei Monaten jede Klinik oder Fabrik vollständig abzusichern. Das Paket liefert deshalb ergebnisbezogene Meilensteine: Verantwortlichkeiten geklärt, Systemgrenze erhoben, kritische Kontrollen geprüft, Ersatzbetrieb geübt, Wiederanlauf belegt und Ausnahmen entschieden.

Jeder Meilenstein hat Eigentümer, erforderliche Evidenz und eine Entscheidung bei Nichterfüllung. Ein Terminverzug führt nicht automatisch zu einer Freigabe aus wirtschaftlichem Druck. Möglich sind engerer Scope, zeitlich begrenzte kompensierende Maßnahmen oder ein Aufschub der neuen autonomen Funktion. Die Entscheidung bleibt transparent und wird nicht in einem Gesamtstatus versteckt.

17. Berichte an Leitung und Aufsicht

Ein Leitungsbericht sollte nicht nur die Anzahl von Angriffen oder abgearbeiteten Tickets zeigen. Er muss beantworten, welche wesentlichen Leistungen wie abhängig sind, welche kritischen Kontrollen nachgewiesen wurden und wo ein nicht akzeptiertes Risiko besteht. Für neue Agenten ist der tatsächlich freigegebene Handlungsspielraum besonders wichtig.

Berichtet werden etwa unbefristete oder überbreite Rechte, fehlende Nachweise kritischer Betriebsmodi, ungeklärte Lieferantenabhängigkeiten, überfällige Ausnahmen und offene Wiederanlaufabgleiche. Die Kennzahlen benötigen Definitionen und dürfen verschiedene Nachweisarten nicht vermischen. „90 Prozent dokumentiert“ ist nicht „90 Prozent technisch geprüft“.

Die Leitung erhält auch Gegenbelege und abweichende Fachmeinungen. Eine belastbare Entscheidung kann einen vertretbaren Restzweifel enthalten; sie darf ihn nicht unsichtbar machen. Ist ein Fachbereich anderer Auffassung, wird der Konflikt mit Begründung und Entscheidung dokumentiert. Das ist besonders wichtig, wenn wirtschaftlicher Nutzen, klinische Versorgung, Datenschutz und technische Eingrenzung unterschiedliche Handlungsrichtungen nahelegen.

18. Wissenschaftliche und fachliche Freigabe dieses Anhangs

Vor Verwendung als verbindliche organisationsinterne Richtlinie sind mindestens die System- und Rechtsanwendbarkeit, klinische beziehungsweise anlagenbezogene Grenzen und die Normvolltexte zu prüfen. Für eine öffentliche redaktionelle Veröffentlichung sind die Quellenstatus, die zeitabhängigen Daten und die deutliche Kennzeichnung der Fallstudien zu erhalten. Ein professionell gesetztes PDF darf diese offenen Prüfpunkte nicht durch ein uneingeschränktes Gütesiegel ersetzen.

Die fachliche Begutachtung sollte Rollen trennen: Ein klinischer Prüfer beurteilt nicht allein die industrielle Schutzfunktion; ein Security-Prüfer ersetzt nicht die Rechtsprüfung; die Redaktion kann keine Konformitätsbewertung einer Maschine vornehmen. Das gemeinsame Ergebnis kann eine freigegebene Fachpublikation sein, ohne ein Zertifikat für irgendeinen konkreten Betrieb zu behaupten.

Die in diesem Paket enthaltene technische Qualitätskontrolle prüft Struktur, Referenzen, Dateien und nachvollziehbare Konsistenz. Sie ist nicht identisch mit dieser externen Begutachtung. Das ist im Statusblatt ausdrücklich ausgewiesen.

19. Fragen, die ein Ausschuss stellen sollte

Ein Ausschuss kann für jede autonome Funktion eine verantwortliche Stelle und einen nachgewiesenen Wirkungsspielraum verlangen. Er kann nach der aktuell geprüften Rechtsrolle fragen, nach dem letzten durchgängigen Ersatzbetriebstest und nach den Bedingungen eines Widerrufs. Er sollte sich zeigen lassen, welche wichtigste Sicherheitsannahme bislang nur auf einer Herstellerzusage beruht.

Weitere Fragen betreffen den Betriebsalltag: Wer ist nachts entscheidungsbefugt? Welche Ausnahme ist abgelaufen? Wie wird eine neue Modell- oder Werkzeugversion erkannt? Welche Daten werden für die Überwachung zusätzlich gespeichert? Welche gesetzliche Meldefrist startet durch welchen Kenntnisstand? Wo liegt die unabhängige fachliche Freigabe für den Wiederanlauf?

Die Qualität der Antwort liegt in auffindbaren Nachweisen, nicht in möglichst umfangreichen Präsentationen. Ein einziger ungeklärter kritischer Pfad kann eine begrenzte Freigabe verhindern; zugleich können viele unkritische offene Punkte die bereits belegte Sicherheit eines anderen Funktionsumfangs unberührt lassen. Deshalb wird nicht mit einem undifferenzierten Gesamtscore entschieden.

20. Arbeitsunterlagen und Ergebnis

Die Kontrollen **K39–K48** bilden den Governance-Kern. **F06 Rollen und Rechtsanwendbarkeit, F09 Reaktionsmandat, F12 Lieferantennachweise, F13 Meldeentscheidungen, F14 Ausnahme, F16 Ausschussentscheidung** und das Quellenregister gehören zur Entscheidungsakte. Die Aktualitäts- und Rechtsprüfung ist vor operativer Anwendung zu dokumentieren.

Ergebnis: Neue Gremien und Berufsbezeichnungen sind nicht das eigentliche Ziel. Die Organisation benötigt eine belastbare Funktion: Sie muss entscheiden können, welche Autonomie sie zulässt, welche Nachweise sie verlangt, welche Risiken sie nicht akzeptiert und wer bei Vertrauensverlust die Handlungsfähigkeit verantwortet.

<!-- GENERATED_LOCAL_BIBLIOGRAPHY -->

Literatur und Quellenstatus

Die folgenden Angaben gehören zu diesem Band. Das vollständige Quellenregister erläutert Verwendungszweck und Zugriff. Quellenstatus und Grenzen sind bei jeder Weiterverwendung zu erhalten. Die Q-Nummern im Text beziehen sich auf diese Einträge; Fundstellen bezeichnen die externe Quelle, nicht eine erfundene PDF-Seite dieses Bandes.

Q04 – NIST. The NIST Cybersecurity Framework (CSF) 2.0. 2024-02-26. DOI: 10.6028/NIST.CSWP.29. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Abstract; Funktionen GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER. Zugriff: Offizielle Publikationsseite und Beschreibung gelesen. Grenze: Rahmenwerk mit Ergebnissen, keine universelle Implementierungsvorschrift und keine eigene Zertifizierung dieses Pakets.

Q22 – Medical Device Coordination Group / Europäische Kommission. MDCG 2019-16 rev. 1: Guidance on Cybersecurity for medical devices. 2020-07 (Rev. 1). [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Abschnitte zu Design / Post-market; Annex IV, gedruckte S. 46. Zugriff: Relevante PDF-Abschnitte gelesen; Inhaltsverzeichnis und Annex IV visuell geprüft. Grenze: Leitlinie ist ausdrücklich nicht rechtsverbindlich; kein Ersatz für MDR/IVDR oder den Normvolltext.

Q29 – Bundesrepublik Deutschland / Gesetze im Internet. BSI-Gesetz (BSIG 2025), aktuelle bereitgestellte Fassung. Gesetz 2025; Änderungsstand im Abruf 2026. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: § 28 und Anlagen: Scope; § 30: Risikomanagement; § 31: kritische Anlagen; § 32: Meldung; § 38: Geschäftsleitung. Zugriff: Bereitgestellter Volltext; §§ 28, 30–32, 38–39 und Änderungsvermerk gelesen. Grenze: Keine automatische Einstufung eines konkreten Unternehmens. Gesetze-im-Internet-Fassung enthält Bearbeitungshinweise; Einzelfall und Spezialregeln separat prüfen.

Q30 – Bundesrepublik Deutschland / Gesetze im Internet. SGB V § 391 – IT-Sicherheit in Krankenhäusern. aktuelle Fassung abgerufen 2026-09-25. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Absätze 1–5; besonders Abs. 5. Zugriff: Vollständiger Paragraph gelesen. Grenze: Keine Gleichsetzung aller Krankenhäuser mit Betreibern kritischer Anlagen; Abgrenzung nach Abs. 5 beachten.

Q31 – Bundesrepublik Deutschland / Gesetze im Internet. Betriebssicherheitsverordnung § 3 – Gefährdungsbeurteilung. aktuelle Fassung abgerufen 2026-09-25. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Abs. 1–3 sowie Aktualisierung / Dokumentation. Zugriff: Paragraph vollständig gelesen. Grenze: Konkrete Prüfpflichten und befähigte Personen aus weiteren Vorschriften und Anlagenscope ableiten, nicht allein aus diesem Paragraphen.

Q32 – Bundesrepublik Deutschland / Gesetze im Internet. Betriebsverfassungsgesetz § 87 – Mitbestimmungsrechte. aktuelle Fassung abgerufen 2026-09-25. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Abs. 1 Nr. 6 und 7. Zugriff: Paragraph gelesen. Grenze: Betriebliche Anwendbarkeit und gesetzliche/tarifliche Vorrangregelungen prüfen; öffentliche und kirchliche Träger können anderen Vertretungsregeln unterliegen.

Q33 – Europäische Kommission, DG CONNECT. AI Act – Application timeline and implementation. Webupdate 2026-08-03. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Application timeline; How has the Commission simplified the implementation of the AI Act?. Zugriff: Aktuelle Webseite einschließlich Omnibus- und Fristenabschnitt gelesen. Grenze: Amtliche Erläuterung ersetzt nicht konsolidierten Normtext. Dessen Abruf war technisch blockiert; rechtsverbindliche Subsumtion bleibt Freigabeaufgabe.

Q34 – Europäische Kommission, DG CONNECT. AI Omnibus enters into force. 2026-07-27. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Entry into force / transition periods. Zugriff: Webtext gelesen. Grenze: Keine vollständige Normkommentierung; für Übergangs-/Bestandsfälle Q39 im Volltext nachprüfen.

Q35 – Europäische Kommission, DG GROW. Machinery – Machinery Regulation. abgerufen 2026-09-25. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Machinery Regulation; mandatory application date. Zugriff: Webtext / Anwendungsdatum gelesen. Grenze: Kein individueller Bescheid; Produktscope, Umbau und aktuelle konsolidierte Anhänge Q40 separat prüfen.

Q36 – Europäische Kommission, DG CONNECT. Cyber Resilience Act – Implementation. Webupdate 2026-07-27. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Implementation timeline. Zugriff: Webtext / Zeitachse gelesen. Grenze: Produkt- und Rollenprüfung erforderlich; nicht jeder Betreiber ist Hersteller.

Q37 – Europäische Kommission, DG CONNECT. Cyber Resilience Act – Reporting obligations. Webupdate 2026-09-11. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: What are the main rules?; Where should manufacturers submit their notifications?. Zugriff: Webtext vollständig gelesen. Grenze: Aktiv ausgenutzte Schwachstelle und schwerwiegender Vorfall unterscheiden. Kein Ersatz für Einzelfallprüfung des CRA.

Q38 – Europäische Union. Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung. 2016; aktuelle Fassung vor Anwendung prüfen. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Art. 5, 6, 9, 25, 28, 30, 32–35, 38–39, 44 ff.. Zugriff: Direkter Web-Volltextabruf technisch blockiert; nicht als neu volltextverifiziert ausgewiesen. Grenze: Artikelzuordnung dient der rechtlichen Prüfung. Redaktionell bekannte Regelungsinhalte werden nicht als vollständig neu geprüfte konsolidierte Rechtsberatung ausgegeben.

Q39 – Europäische Union. AI Act, Verordnung (EU) 2024/1689 – konsolidierte Fassung vom 27.07.2026. 2026-07-27. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Art. 6, 9–15, 26, 113; Anhänge I/III; Änderungsverordnung EU 2026/1744. Zugriff: Abruf technisch blockiert; aktuelle Zeitachse über Q33/Q34 geprüft. Grenze: Keine Behauptung, der konsolidierte Volltext sei in dieser Recherche geprüft worden. Geänderte Detailvorschriften vor konkreter Nutzung juristisch lesen.

Q40 – Europäische Union. Verordnung (EU) 2023/1230 – Maschinenverordnung. 2023; konsolidierte Fassung vor Anwendung prüfen. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Anwendungs-/Übergangsbestimmungen; Anhang III insbesondere 1.1.9 und 1.2.1 als Prüfsuchstellen. Zugriff: Volltextabruf technisch blockiert; Datum/Überblick über Q35 geprüft. Grenze: Fundstellen sind Suchaufträge für die aktuelle Volltextprüfung, kein behaupteter vollständiger Nachweis sämtlicher Anforderungen.

Q41 – Europäische Union. Verordnung (EU) 2024/2847 – Cyber Resilience Act. 2024; Anwendungsstufen bis 2027. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Art. 2 Scope; Art. 14–16 Meldung; Art. 24 Software-Stewards; Art. 71 Fristen. Zugriff: Volltextabruf technisch blockiert; aktuelle Übersicht und Berichtspflichten Q36/Q37 gelesen. Grenze: Ausnahmen, unter anderem sektoral regulierte Produkte, müssen am aktuellen Normtext einzeln bestätigt werden.

Arbeitsmittel: Kontrollkatalog, Formularbuch, Fallstudien und Claim–Evidence–Matrix.

12 Rechtliche Hinweise

12.1 Keine Beratung

Diese Veröffentlichung ist ein redaktionelles Erzeugnis. Sie stellt keine Rechtsberatung, keine medizinische, pflegerische, arbeitsrechtliche oder datenschutzrechtliche Beratung und keine Beschaffungs- oder Vergabeberatung dar. Sie ersetzt insbesondere nicht die Prüfung durch Rechtsanwaltschaft, Datenschutzaufsicht, Medizinprodukteberatung, Vergabestelle, Ethikkommission nach Medizinprodukterecht oder Arbeitnehmervertretung. Wer auf Grundlage dieses Dokuments entscheidet, entscheidet auf eigene Verantwortung und hat den Sachverhalt vorher eigenständig fachlich prüfen zu lassen.

12.2 Keine Zusicherung, keine Konformitätsaussage

Die beschriebenen Verfahren, Prüfstufen und Checklisten sind redaktionelle Vorschläge. Sie sind keine Zusicherung einer Eigenschaft, kein garantiertes Ergebnis und kein Nachweis der Einhaltung einer Rechtsvorschrift. Wer ein Verfahren aus diesem Dokument anwendet, erfüllt damit keine gesetzliche Anforderung; ob eine Anforderung erfüllt ist, entscheidet die zuständige Stelle am Einzelfall.

12.3 Rechtsstand

Rechtsstände, Fristen und Fundstellen beziehen sich auf den im Dokumentkopf genannten Tag. Der KI-Rechtsrahmen wird laufend geändert; ein älterer Fristenplan darf nicht unverändert weiterverwendet werden. Genannte Gesetze und Verordnungen sind in ihrer jeweils geltenden Fassung heranzuziehen.

12.4 Haftung

Die Inhalte wurden mit Sorgfalt erstellt und, soweit im Methodenteil beschrieben, gegengeprüft. Für Richtigkeit, Vollständigkeit und Aktualität wird gleichwohl keine Gewähr übernommen. Eine Haftung des Herausgebers ist auf Vorsatz und grobe Fahrlässigkeit beschränkt; dies gilt nicht bei der Verletzung des Lebens, des Körpers oder der Gesundheit sowie bei zwingender gesetzlicher Haftung.

12.5 Verweise auf fremde Inhalte

Dieses Dokument verweist auf Inhalte Dritter, insbesondere auf Behörden-, Fachgesellschafts-, Normen- und Fachverlagsseiten. Auf deren Gestaltung und Inhalt hat der Herausgeber keinen Einfluss; für sie ist jeweils der dortige Anbieter verantwortlich. Die Adressen waren zum im Literaturverzeichnis genannten Prüfzeitpunkt erreichbar. Die Nennung eines Produkts, Herstellers oder Dienstes ist weder eine Empfehlung noch eine Bewertung seiner Eignung.

12.6 Marken und Produktbezeichnungen

Genannte Produkt-, Marken- und Unternehmensbezeichnungen sind Kennzeichen ihrer jeweiligen Inhaber und werden ausschließlich zur Beschreibung des Sachverhalts verwendet. Aus der Nennung folgt keine Verbindung zwischen dem Herausgeber und dem jeweiligen Unternehmen und keine Aussage über Zulassungs-, Konformitäts- oder Zertifizierungsstatus.

12.7 Urheberrecht und Nutzung

Dieses Dokument, sein Text, seine Tabellen und seine Abbildungen sind urheberrechtlich geschützt. Rechteinhaberin ist die WebTrades GmbH. Zulässig sind das Lesen, das Speichern und der Ausdruck für den eigenen Gebrauch sowie das Zitieren einzelner Stellen mit vollständiger Quellenangabe nach der im Impressum genannten Zitierweise. Die Vervielfältigung, Bearbeitung, Verbreitung, öffentliche Zugänglichmachung oder kommerzielle Verwertung des Dokuments oder wesentlicher Teile daraus bedarf der vorherigen schriftlichen Zustimmung der Rechteinhaberin. Das gilt ausdrücklich auch für die Übernahme von Tabellen und Abbildungen.

12.8 Keine personenbezogenen Daten

Für dieses Dokument wurden keine personenbezogenen Daten verarbeitet. Es beruht auf veröffentlichter Literatur, amtlichen Rechtsquellen und Veröffentlichungen von Fachgesellschaften; es wurden weder Beschäftigte befragt noch Patientendaten verwendet. Wer die hier beschriebenen Verfahren auf eine reale Einrichtung anwendet, verlässt diesen Rahmen: Die Auswertung von Tätigkeits-, Alarm- oder Quittierungsdaten unterliegt der Datenschutz-Grundverordnung und in der Regel der Mitbestimmung.

12.9 Unabhängigkeit

Dieses Dokument ist ohne Auftrag, ohne Finanzierung und ohne inhaltliche Beteiligung eines Herstellers, Krankenhausträgers, Kostenträgers, Verbands oder Beratungsunternehmens entstanden. Es besteht kein Vergütungs- oder Beteiligungsverhältnis zu einem der genannten Unternehmen oder Institutionen. Genannt werden Systeme, Anbieter und Dokumente, weil sie in den beschriebenen Gegenstand fallen, nicht weil sie beworben werden sollen.

12.10 Anwendbares Recht

Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts. Gesetzliche Verbraucherschutzvorschriften bleiben unberührt.