

Datenrechte, regulatorische Einordnung, Cybersicherheit und kontrollierte Updates

Entscheidungsziel: Für eine konkrete Anwendung feststellen, wer welche Pflichten trägt, welche Daten zu welchem Zweck verwendet werden dürfen und unter welchen Bedingungen Änderungen zulässig sind.

Fassung 1.0 · Recherchestichtag 25. September 2026 · Adressaten: Rechts- und Compliance-Funktionen, Datenschutzbeauftragte, Informationssicherheit, IT/OT, Produktverantwortliche, Hersteller und Betreiber.

Dokumenttyp: strukturierte integrative Recherche mit abgeleiteten Verfahren, keine systematische Übersichtsarbeit, keine eigene empirische Robotikstudie und keine einzelfallbezogene Rechts- oder Förderberatung.

Eine unabhängige Begutachtung, Zertifizierung oder fallbezogene Rechtsberatung ist mit der Erstellung dieses Leitfadens nicht erfolgt.

Steckbrief

Merkmal	Wert
Dokumenttyp	Strukturierte integrative Recherche mit abgeleiteten Verfahren; keine systematische Übersichtsarbeit, keine unabhängige Fachbegutachtung
Zielgruppe	Rechts- und Compliance-Funktionen, Datenschutzbeauftragte, Informationssicherheit, IT/OT, Produktverantwortliche, Hersteller und Betreiber.
Recherche- und Rechtsstand	25. September 2026
Umfang	4.386 Wörter, 16 Seiten
Belege	0 Literatureinträge, 21 Quellenadressen
Gliederung	14 nummerierte Abschnitte, 2 Tabellen

Inhalt

1. Rechtsprüfung und technische Architektur gehören zusammen	5
2. Verifizierter Rechtsstand und dokumentierte Zugriffsgrenzen	5
3. Eine anwendungsbezogene Rechtsakte aufbauen	5
4. Die besondere AI-Act-Schnittstelle für Maschinen	6
5. Datenrechte nicht als Eigentumsfrage verkürzen	6
5.1 Vier verschiedene Rechtsfragen	6
5.2 Rollen sind pro Datenfluss zu bestimmen	7
5.3 Datenkategorien sachgerecht abgrenzen	7
6. Aus Datenzugang wird nicht automatisch Trainingsrecht	7
7. Datenschutz im physischen Raum	8
8. Datenflussmatrix und kontrollierte Freigabe	8
9. Cybersicherheit als Eigenschaft des Gesamtsystems	8
10. CRA: Produktpflichten und Betrieb nicht verwechseln	9
11. Änderungen als geschlossene Nachweiskette behandeln	9
11.1 Zwischen Protokollierung und Lernen unterscheiden	9
11.2 Was eine Änderungsakte enthalten sollte	10
11.3 Rollback mit Sicherheits- und Rechtsbezug	10
12. Ein Incident-Verfahren, das physische und digitale Folgen verbindet	10
13. Vertragliche Gestaltung: prüfbare Inhalte statt Musterklauseln	10
14. Abnahme einer Daten- und Änderungsarchitektur	11
Quellen zu diesem Dokument	11
Q014 · RoX-Konsortium	11
Q017 · Boston Dynamics	11
Q022 · NIST	11
Q023 · NIST	12
Q026 · Europäische Kommission / DG CONNECT	12
Q027 · Europäisches Parlament und Rat	12
Q028 · Europäische Kommission / DG GROW	12
Q029 · Europäische Kommission / DG CONNECT	12
Q030 · Europäisches Parlament und Rat	12
Q031 · Europäische Kommission / DG CONNECT	12
Q032 · Europäische Kommission / DG CONNECT	13
Q033 · Europäisches Parlament und Rat	13
Q034 · Europäischer Datenschutzausschuss	13
Q035 · Europäisches Parlament und Rat	13
Q037 · Medical Device Coordination Group (MDCG)	13
Q039 · Bundesministerium der Justiz / Gesetze im Internet	13
Q040 · Europäische Kommission / DG CONNECT	14
Q041 · Autoriteit Consument & Markt (ACM), Niederlande	14

12 Rechtliche Hinweise 15

12.1 Keine Beratung	15
12.2 Keine Zusicherung, keine Konformitätsaussage	15
12.3 Rechtsstand	15
12.4 Haftung	15
12.5 Verweise auf fremde Inhalte	15
12.6 Marken und Produktbezeichnungen	15
12.7 Urheberrecht und Nutzung	15
12.8 Keine personenbezogenen Daten	16
12.9 Unabhängigkeit	16
12.10 Anwendbares Recht	16

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): *Datenrechte, regulatorische Einordnung, Cybersicherheit und kontrollierte Updates*. 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. Rechtsprüfung und technische Architektur gehören zusammen

Bei Physical AI können Daten- und Softwareentscheidungen unmittelbar beeinflussen, wie sich ein physisches System verhält. Ein neues Trainingsverfahren, ein zusätzlicher Cloudzugriff oder eine veränderte Sensorauswertung ist deshalb nicht nur eine IT-Frage. Es kann Zweckbestimmung, Sicherheit, personenbezogene Daten, Vertragsbeziehungen und die Reichweite bisheriger Nachweise berühren.

Dieser Leitfaden liefert eine **Prüfroute**, keine verbindliche Einzelfallklassifikation. Er trennt gesetzliche Fundstellen, behördliche Erläuterungen und eigene organisatorische Empfehlungen. Nicht jeder Roboter fällt unter dieselben Regelungen. Ein industrieller Materialtransport, ein medizinisches Assistenzsystem und eine Software zur Bewertung von Beschäftigten können trotz gemeinsamer technischer Komponenten unterschiedlichen Pflichten unterliegen.

Die Prüfung beginnt mit Produkt, Funktion, Markt, Rolle und Zeitpunkt. Erst dann werden Rechtsakte zugeordnet. Eine Tabelle mit Gesetzesnamen ohne diese Zuordnung erzeugt Scheinsicherheit: Sie sagt weder, wer verpflichtet ist, noch welche Dokumente tatsächlich benötigt werden. Ebenso wenig genügt die Aussage „Wir sind nur Betreiber“, wenn die Organisation selbst wesentliche Änderungen vornimmt oder unter eigenem Namen ein Produkt bereitstellt. Die Rollenfolge muss an der konkreten Gestaltung geprüft werden.

2. Verifizierter Rechtsstand und dokumentierte Zugriffsgrenzen

Die allgemeine Anwendung der Maschinenverordnung (EU) 2023/1230 beginnt am **20. Januar 2027**. Die Kommission erläutert zugleich die Abgrenzung zum bis dahin maßgeblichen Maschinenrichtlinienregime und weist auf Konformitätsverfahren und irreführende freiwillige Zertifikate hin. [Q028, Machinery Regulation / Compliance and conformity]

Der AI-Omnibus-Rechtsakt **(EU) 2026/1744** verändert nicht nur Termine. Er verlagert die Maschinenverordnung in Anhang I Abschnitt B des AI Act und verändert den sektoralen Umsetzungsweg. Für produktbezogene Hochrisiko-KI nach Artikel 6 Absatz 1 ist der 2. August 2028 eine zentrale Zeitmarke; für die maschinenbezogene Fallgruppe müssen jedoch der geänderte Artikel 2 Absatz 2 und die sektoralen Änderungen mitgelesen werden. Ein pauschales „ab 2028 gelten für jeden Roboter alle Hochrisikopflichten des AI Act unmittelbar identisch“ wäre falsch. [Q027, Art. 1 Nr. 2, 40–41 und Art. 3; Q026, Anwendungskalender]

Der Data Act gilt grundsätzlich seit **12. September 2025**. Die besondere Gestaltungspflicht für den Datenzugang nach Artikel 3 Absatz 1 betrifft verbundene Produkte und verbundene Dienste, die **nach dem 12. September 2026** in Verkehr gebracht werden. Allgemeiner Datenzugang und diese spätere Designverpflichtung sind auseinanderzuhalten. [Q029, Einführung/Kapitel II; Q030, Art. 3 und 50; Q041, Abschnitt 2.3, Rn. 32–33]

Beim CRA gelten bestimmte Herstellermeldepflichten seit **11. September 2026**; die allgemeinen Hauptpflichten folgen am **11. Dezember 2027**. Die konkrete Rolle und Produktkategorie bleiben entscheidend. [Q031, Main rules; Q042, Application timeline]

Bei mehreren Rechtsakten war der direkte EUR-Lex-Abruf in dieser Arbeitsrunde technisch blockiert. Die amtlichen Erläuterungen wurden geprüft; der AI-Omnibus-Änderungstext wurde zusätzlich in einer zugänglichen Amtsblatt-Spiegelkopie gelesen und visuell kontrolliert. Das Register legt dies pro Quelle offen. Vor Vertrags-, Konformitäts- oder Betriebsfreigabe muss die verantwortliche Rechtsfunktion den aktuellen Originalstand einschließlich Änderungen sichern. Der Leitfaden behauptet keine vollständige unabhängige Rechtsprüfung sämtlicher Sektoren.

3. Eine anwendungsbezogene Rechtsakte aufbauen

Die Rechtsakte beginnt mit einer nüchternen Funktionsbeschreibung. Sie enthält bestimmungsgemäßen Einsatz, betroffene Personen, autonome und menschliche Entscheidungen, physische Aktoren, erforderliche Dienste und vorgesehene Änderungen. Marketingbezeichnungen wie „Assistent“, „Plattform“ oder „nur KI“ ersetzen diese Beschreibung nicht.

Prüfpfad	Eingangsdaten	Erwartetes Ergebnis	Fundstelle
Maschinen-/Produktsicherheit	Produkt, Funktion, Bereitstellung, wesentliche Änderungen, Markt	Anwendbares Produktregime und verantwortliche Rolle	Q028; sektorale Änderungen Q027
Arbeitgeber/Betrieb	Arbeitsmittel, Standort, Organisation und Störungen	Fachkundige Gefährdungsbeurteilung und Prüfplanung	Q039, § 3 BetrSichV
AI Act	Konkrete KI-Funktion, Rolle als Sicherheitskomponente, weiterer Verwendungszweck	Dokumentierte Einstufung und passender unmittelbarer/sektoraler Pfad	Q026; Q027
Data Act	Verbundenes Produkt/Dienst, Nutzer, Dateninhaber, Datenkategorien	Zugangs- und Nutzungsrechte einschließlich Ausnahmen	Q029–Q030; Q041
Datenschutz	Identifizierbare Personen, Zwecke, Rollen, Empfänger, Übermittlungen	Rechtsgrundlagen, Schutzmaßnahmen und gegebenenfalls Folgenabschätzung	Q034–Q035
CRA	Digitales Produkt, Bereitstellung, Vernetzung, Rolle und Ausnahmen	Zeitabhängige Produkt-, Support- und Meldepflichten	Q031–Q033; Q040; Q042
Medizinischer Zweck	Zweckbestimmung von Hardware, Software und Zubehör	Gesonderte MDR-/IVDR-Prüfung	Q037; L07

Nicht jede Zeile führt automatisch zu einer Pflicht. Ein begründet ausgeschlossener Anwendungsbereich wird mit der tragenden Annahme dokumentiert. Ändert sich diese Annahme, wird die Einordnung erneut geöffnet. Der Prozess darf nicht bei einer einmaligen juristischen Bewertung stehen bleiben, wenn das Produkt später neue Funktionen erhält.

4. Die besondere AI-Act-Schnittstelle für Maschinen

Der geänderte Artikel 2 Absatz 2 des AI Act begrenzt für bestimmte nach Artikel 6 Absatz 1 hochriskante Systeme im Bereich des Anhangs I Abschnitt B die unmittelbar anwendbaren Vorschriften. Parallel verpflichtet die Änderung der Maschinenverordnung die Kommission zu sektoraler Ergänzung wesentlicher Anforderungen. Diese Ergänzungen sollen bis 2. August 2028 gelten. Die konkrete maschinenbezogene Rechtsroute muss daher als Zusammenspiel von AI Act und Maschinenverordnung dokumentiert werden, nicht als bloße Verschiebung eines unveränderten Pflichtenpakets. [Q027, Amtsblattseiten 15–16, 36–37 und 40–41]

Für eine Organisation bedeutet dies praktisch: Sie beschreibt zunächst, ob die betrachtete KI eine sicherheitsbezogene Rolle im Produkt besitzt und welcher Rechtsakt das Produkt erfasst. Danach werden etwaige zusätzliche KI-Anwendungen getrennt betrachtet. Eine Funktion zur Personalbewertung oder eine eigenständige medizinische Auswertung wird nicht allein deshalb identisch behandelt, weil dieselbe Hardwareplattform Daten liefert.

Der Begriff „Hochrisiko“ ist keine pauschale Charakterisierung eines Unternehmens und kein Synonym für einen gefährlich aussehenden Roboter. Er bezeichnet eine rechtliche Einstufung anhand konkreter Voraussetzungen. Ebenso wenig beweist die Trennung einer KI von einer Sicherheitssteuerung automatisch, dass alle AI-Act-Fragen erledigt sind. Zweck, Funktion und Auswirkungen müssen tatsächlich untersucht werden.

Die technische Konsequenz ist eine versionierte Zuordnung von Anforderungen und Nachweisen. Solange sektorale Detailanforderungen noch konkretisiert werden, kann eine Entwicklungsorganisation bereits Datenherkunft, Risikomanagement, Protokollierung, Robustheit und Änderungsbeherrschung dokumentieren. Sie muss dabei klar unterscheiden, welche Maßnahmen heute verbindlich, vertraglich zugesagt oder vorsorglich fachlich sinnvoll sind.

5. Datenrechte nicht als Eigentumsfrage verkürzen

5.1 Vier verschiedene Rechtsfragen

Die Frage „Wem gehören die Roboterdaten?“ ist für die Praxis zu grob. Getrennt zu prüfen sind Zugang, Nutzung, Weitergabe und Rechte an daraus entstehenden Ergebnissen. Eine Organisation kann Zugriff auf Daten besitzen, ohne sie für allgemeines Modelltraining verwenden zu dürfen. Eine andere kann bestimmte Ergebnisse kommerziell nutzen, ohne sämtliche Rohdaten offenlegen zu müssen.

Der Data Act betrifft unter anderem Daten aus verbundenen Produkten und Diensten. Die Kommission nennt ausdrücklich auch Roboter und industrielle Maschinen. Er schafft keine universelle Eigentumsordnung für sämtliche Daten und verdrängt die Datenschutzregeln nicht. Für die Anwendung sind Rollen und Datenkategorien entscheidend. [Q029, Kapitel II; Q030, Art. 2–6]

5.2 Rollen sind pro Datenfluss zu bestimmen

Beim gleichen System können Hersteller, Integrator, Betreiber, Cloudanbieter und Modellanbieter unterschiedliche Funktionen übernehmen. Der rechtliche Nutzer eines verbundenen Produkts ist nicht notwendigerweise jede Person, die es bedient. Insbesondere kann eine Organisation Nutzer sein, während Beschäftigte als betroffene Personen eigene Datenschutzrechte haben. Die vorläufige ACM-Leitlinie erläutert diese Unterscheidung anhand von Eigentums- und nutzungsähnlichen Vertragsrechten. [Q041, Abschnitt 2.4, insbesondere Rn. 36]

Bei Robot-as-a-Service ist die konkrete Vertragsgestaltung maßgeblich. Die bloße Eigentumsposition des Anbieters beantwortet nicht abschließend, welche Rechte dem Kunden zustehen. Umgekehrt folgt aus einer allgemeinen Dienstleistungsbeziehung nicht automatisch jede Eigenschaft eines Miet- oder Leasingnutzers. Die Rechtsakte sollte deshalb die tatsächlichen Nutzungsrechte, Datenflüsse und Zweckentscheidungen dokumentieren.

5.3 Datenkategorien sachgerecht abgrenzen

Ein Inventar unterscheidet Roh- und vorverarbeitete Sensordaten, Metadaten, Betriebsereignisse, Daten aus verbundenen Diensten, abgeleitete Analysen und Modellartefakte. Diese Kategorien dürfen nicht nur nach Dateiendung gebildet werden. Eine umbenannte Rohdatendatei wird dadurch nicht zu einer rechtlich ausgenommenen Analyse. Ebenso ist ein aufwendiges Analyseergebnis nicht automatisch mit seinen Eingangsdaten gleichzusetzen.

Für jede Kategorie werden Entstehung, Verarbeitungsschritte, Verfügbarkeit beim Dateninhaber und Bezug zur Nutzung beschrieben. Der Umfang gesetzlicher Zugangsrechte wird daran geprüft. Die behördlichen Erläuterungen unterscheiden zugängliche Roh- und vorverarbeitete Daten von bestimmten abgeleiteten beziehungsweise inferierten Ergebnissen. Die technische Dokumentation muss diese Abgrenzung nachvollziehbar machen. [Q029, Types of data in scope; Q041, Abschnitt 4.5]

6. Aus Datenzugang wird nicht automatisch Trainingsrecht

Ein realistischer Vertrag trennt mindestens Betrieb, Diagnose, Wartung, anwendungsspezifische Verbesserung und allgemeines Modelltraining. Der technische Nutzen zusätzlicher Daten kann hoch sein; die Zulässigkeit folgt jedoch nicht aus diesem Nutzen. Eine Vertragsklausel zur Fehlerdiagnose sollte nicht stillschweigend als Freigabe für ein branchenübergreifendes Foundation Model interpretiert werden.

Bei personenbezogenen Daten sind zusätzlich Zweck, Rechtsgrundlage und Rollen nach Datenschutzrecht zu prüfen. Die EDPB-Leitlinie stellt auf tatsächliche Zwecke und Mittel ab. Ein Anbieter, der für eigene Zwecke über die Verarbeitung entscheidet, kann nicht allein durch die Überschrift „Auftragsverarbeiter“ von dieser Rolle entbunden werden. Gemeinsame Verantwortlichkeit und Auftragsverarbeitung sind anhand der tatsächlichen Zusammenarbeit abzugrenzen. [Q034, Teil I und II]

Für nicht personenbezogene Daten bleiben unter anderem Vertragsrechte, Data-Act-Vorgaben, Geschäftsgeheimnisse und Rechte Dritter relevant. Auch gesetzlich eröffneter Zugang ist nicht grenzenlose Nutzung. Eine Rechteakte sollte deshalb ausdrücklich festhalten, ob Daten zu einem konkreten Modell, für eine Aufgabe oder für weitergehende Produkte verwendet werden dürfen. Beschränkungen für die Entwicklung konkurrierender verbundener Produkte und andere gesetzliche Grenzen werden an der konkreten Empfängerrolle geprüft. [Q030, Art. 4–6; Q041, Abschnitt 5]

Die operative Empfehlung lautet: Jeder Trainingslauf erhält einen Verweis auf die zulässigen Zwecke und zugelassenen Datenbestände. Damit wird die Rechtsprüfung technisch anschlussfähig. Eine spätere Nachkontrolle kann nachvollziehen, welches Modell mit welchen Daten unter welcher Berechtigung entstanden ist. Das ist eine empfohlene Governance-Maßnahme, keine Behauptung, jeder Trainingslauf müsse gesetzlich in genau diesem Format dokumentiert werden.

7. Datenschutz im physischen Raum

Roboterdaten können Personen direkt oder indirekt identifizierbar machen. Kamerabilder, Sprachaufzeichnungen, Laufwege oder Zeitstempel können einen Personenbezug erhalten, auch wenn kein Name gespeichert wird. Umgekehrt ist nicht jede technische Messgröße automatisch personenbezogen. Die Einordnung hängt vom Kontext und den realistisch verfügbaren Verknüpfungsmöglichkeiten ab. [Q035, Art. 4–6 als juristische Fundstellen; Q041, Rn. 40]

Eine datensparsame Architektur fragt, welche Informationen für die konkrete Funktion tatsächlich benötigt werden. Für eine technische Störungsanalyse können begrenzte Ausschnitte, reduzierte Merkmale oder ereignisbezogene Aufzeichnungen genügen. Solche Maßnahmen müssen auf ihre Wirksamkeit geprüft werden. Verpixelung oder das Entfernen von Namen ist nicht automatisch belastbare Anonymisierung; die verbleibende Identifizierbarkeit ist zu untersuchen.

Für Beschäftigte und insbesondere Patientinnen und Patienten sind zusätzliche Interessen zu berücksichtigen. Eine pauschale Einwilligung wird nicht als allgemeines Heilmittel empfohlen. Rechtsgrundlagen, Informationspflichten, besondere Datenkategorien, Beteiligungsrechte und gegebenenfalls eine Datenschutz-Folgenabschätzung werden mit den zuständigen Stellen geprüft. Die wesentlichen Fundstellen sind in Q035 benannt; eine vollständige arbeits- oder gesundheitsrechtliche Einzelfallprüfung ist nicht Bestandteil dieses Pakets.

Eine Folgenabschätzung ist nicht nur ein Dokument nach Fertigstellung der Architektur. Sie sollte bei voraussichtlich hohem Risiko früh genug einbezogen werden, damit Alternativen noch möglich sind. Die organisatorische Empfehlung ist, Datenschutzfragen gemeinsam mit Sensorik, Speicherung, Fernzugriff und Training zu bearbeiten, statt sie in einen späteren Freigabeschritt zu verschieben.

8. Datenflussmatrix und kontrollierte Freigabe

Für jeden Datenstrom werden Quelle, Inhalt, Zweck, Empfänger, Übertragungsweg, Speicherort, Aufbewahrung, Zugriffsrechte und Lösch- beziehungsweise Sperrmechanismus dokumentiert. Die Matrix unterscheidet Produktion, Support, Forschung und Training. Ein gemeinsamer Datensee ohne solche Zweckgrenzen erschwert spätere Kontrolle.

Datenstrom im eigenen Beispielfall	Primärer Zweck	Besondere Prüffrage	Empfohlene Begrenzung
Zustands- und Temperaturwerte	Betrieb/Diagnose	Welche Daten sind für Kunden und Service zugänglich?	Zweckbezogene Schnittstelle und Datenwörterbuch
Kamerabild bei Störung	Ursachenanalyse	Personen, Geschäftsgeheimnisse, unnötiger Hintergrund?	Ereignisbezug, Zugriffsbeschränkung, begründete Aufbewahrung
Annotierte Fehlerszenen	Verbesserung einer konkreten Aufgabe	Reicht die bestehende Erlaubnis für Annotation und Training?	Getrennte Freigabe und dokumentierte Herkunft
Flottenübergreifender Trainingsbestand	Allgemeine Modellverbesserung	Weitergehender Zweck, Rechte Dritter und Drittlandzugriffe?	Eigenständige Rechts- und Sicherheitsprüfung
Update- und Freigabelog	Nachvollziehbarkeit	Integrität, Personenbezug, benötigte Aufbewahrung?	Geschütztes Rollenmodell und versionierte Protokolle

Diese Tabelle beschreibt ein hypothetisches Design, keine allgemeine Erlaubnis. Jeder reale Datenstrom benötigt seine eigene Prüfung. Besonders wichtig ist die technische Durchsetzung: Eine vertragliche Beschränkung bleibt schwach, wenn sämtliche Daten standardmäßig für alle Entwickler und externe Dienstleister zugänglich sind.

RoX demonstriert eine Architekturidee, in der Datenaustausch und Modellverbesserung mit Nachvollziehbarkeit und Datenkontrolle verbunden werden. Daraus folgt keine automatische Rechtskonformität jeder Umsetzung. Der nützliche Grundgedanke ist, Rechte und Datenverwendung bereits in die Infrastruktur einzubauen. [Q014, AI ecosystem / traceability]

9. Cybersicherheit als Eigenschaft des Gesamtsystems

Die Bedrohungsanalyse umfasst Gerät, lokale Netze, Cloud, Fernwartung, Identitäten, Trainings- und Lieferkette. Bei Physical AI ist nicht allein Datenverlust relevant. Unberechtigte Änderungen können auch Verfügbarkeit, Qualität oder physisches Verhalten beeinflussen. Welche Auswirkungen möglich sind, muss an der konkreten Architektur untersucht werden.

Sinnvolle Schutzprinzipien sind begrenzte Berechtigungen, nachvollziehbare Identitäten, abgesicherte Kommunikationswege, kontrollierte Fernzugriffe, segmentierte Verantwortungsbereiche und überprüfbare Wiederherstellung. Diese Prinzipien sind keine Aufforderung, Schutzmaßnahmen ohne Kenntnis des Betriebs auf bestehende Maschinen aufzusetzen. Änderungen in der OT können selbst Verfügbarkeit und Sicherheit beeinflussen und müssen entsprechend geplant werden. NIST SP 800-82 liefert hierfür eine technische Referenz. [Q022]

Bei lernenden Systemen ist zusätzlich zu fragen, welche Inhalte Handlungen beeinflussen können. Eine natürliche Spracheingabe, ein Dokument oder ein visuell wahrgenommener Text kann in manchen Architekturen Teil der Entscheidungsgrundlage werden. Die defensive Prüfung untersucht daher Vertrauensgrenzen: Welche Eingaben sind Daten, welche dürfen Anweisungen auslösen, und welche Handlungsmöglichkeiten sind technisch begrenzt? Der Leitfaden beschreibt keine Angriffsdurchführung, sondern die zu dokumentierende Sicherheitsfrage.

Drittkomponenten werden mit Version, Herkunft und Verantwortlichkeit erfasst. Eine Softwarestückliste allein ist noch kein Schwachstellenmanagement; sie macht lediglich bestimmte Abhängigkeiten auffindbar. Ebenso kann eine Modellkarte die Herkunft beschreiben, ohne Manipulationsfreiheit zu garantieren. NIST SSDF ergänzt die Perspektive um sichere Entwicklung und Behandlung erkannter Schwachstellen. [Q023]

10. CRA: Produktpflichten und Betrieb nicht verwechseln

Der CRA adressiert Produkte mit digitalen Elementen und differenzierte Rollen in der Lieferkette. Vor einer Anwendung auf Robotik werden Marktbereitstellung, Vernetzung und mögliche sektorale Ausnahmen geprüft. Gerade bei medizinischen Produkten ist die Abgrenzung zum besonderen Produktrecht ausdrücklich zu untersuchen; eine pauschale Addition aller Regime ist nicht sachgerecht. [Q032, Chapter I; Q033, Art. 2 als Originalfundstelle]

Die geprüften Kommissionsinformationen beschreiben Risikobeurteilung, technische Dokumentation, Konformitätsverfahren, Supportangabe und Schwachstellenbehandlung über den relevanten Zeitraum. Für eine Beschaffung folgt daraus die praktische Frage, welcher Support konkret zugesagt ist und wie Sicherheitsinformationen den Betreiber erreichen. Die genaue gesetzlich erforderliche Dauer wird anhand des Produkts und der anwendbaren Vorschriften bestimmt; eine beliebige Standardzahl ersetzt diese Prüfung nicht. [Q040, Before / At / After placing on the market]

Seit 11. September 2026 müssen betroffene Hersteller aktiv ausgenutzte Schwachstellen und schwere Sicherheitsvorfälle nach den einschlägigen CRA-Regeln melden. Die Kommission nennt eine Frühwarnung binnen 24 Stunden und eine vollständige Meldung binnen 72 Stunden ab Kenntnis. Abschlussberichte unterscheiden sich: bei aktiv ausgenutzten Schwachstellen spätestens 14 Tage nach Verfügbarkeit einer Korrekturmaßnahme, bei schweren Vorfällen innerhalb eines Monats nach der 72-Stunden-Meldung. Rolle, Ereignistyp und Beginn der Kenntnis müssen dokumentiert werden. [Q031, What are the main rules?]

Diese Regeln gelten nicht pauschal für jeden Betreiber und jede Betriebsstörung. Ein einziges Ereignis kann allerdings mehrere Prüfpfade auslösen, etwa Produktsicherheit, Datenschutz und Cybersicherheit. Das Incident-Verfahren benötigt deshalb eine Verantwortungs- und Fristenmatrix. Es darf nicht annehmen, dass eine Meldung an eine Stelle alle anderen Pflichten automatisch erfüllt.

11. Änderungen als geschlossene Nachweiskette behandeln

11.1 Zwischen Protokollierung und Lernen unterscheiden

Datenerfassung ist nicht gleich Modelltraining. Offline-Analyse, Offline-Neutraining, Zusammenführung von Flottendaten, kontrollierte Modellverteilung und Online-Anpassung sind verschiedene Prozesse. Für jeden Prozess wird festgelegt, welche Daten verwendet, welche Parameter verändert und welche Freigaben benötigt werden. Die Aussage „Das System lernt ständig“ ist ohne diese Unterscheidung technisch und rechtlich unbrauchbar.

Ein konkretes Herstellerbeispiel zeigt, warum diese Trennung praktisch relevant ist: Die Datenschutzhinweise für Stretch unterscheiden Serviceprotokolle und Leistungsmetriken und beschreiben ihre Verwendung für Analyse und Verbesserung. Das belegt eine bestimmte dokumentierte Herstellerpraxis, nicht dieselbe Datennutzung bei allen Robotern oder die Zulässigkeit jedes Trainingszwecks. [Q017, Service logs / Performance metrics]

Eine kontrollierte Verbesserungskette lautet: Ereignis erfassen, Datenqualität und Rechte prüfen, Änderungshypothese formulieren, Entwicklungsstand erzeugen, unabhängig testen, Auswirkungen bewerten, freigeben, begrenzt ausrollen und Wirkung überwachen. Rückmeldungen aus dem Betrieb können die nächste Forschungsschleife auslösen. Jede dieser Übergaben besitzt einen verantwortlichen Empfänger; sonst gehen entweder Wissen oder Kontrolle verloren.

11.2 Was eine Änderungsakte enthalten sollte

Die Änderungsakte nennt den Anlass, alte und neue Konfiguration, betroffene Anforderungen, Datenherkunft, rechtliche Zweckprüfung, Sicherheitsfolgen, Regressionstests, autorisierte Freigabe und Wiederherstellungsweg. Sie enthält auch die Begründung, warum bestimmte bisherige Nachweise weiterhin gelten. Ein vollständiger Neustart aller Prüfungen ist nicht für jede Änderung nötig; die Reichweite der Wiederverwendung muss jedoch nachvollziehbar sein.

Eine Funktionsverbesserung kann den bisherigen Nutzungskorridor erweitern. Dann reicht ein Vergleich „besser als vorher“ nicht. Die neue Aufgabe benötigt passende Anforderungen und Evidenz. Umgekehrt kann eine Änderung innerhalb eines bereits freigegebenen Korridors liegen. Die Abgrenzung ist fachlich zu prüfen und darf nicht allein aus der Versionsnummer abgeleitet werden.

11.3 Rollback mit Sicherheits- und Rechtsbezug

Ein Rücksprung auf einen früheren Stand ist nur dann ein geeigneter Wiederherstellungsweg, wenn dieser Stand weiterhin zulässig, kompatibel und sicher ist. Ein früheres Modell kann nach einer mechanischen Änderung nicht mehr passen. Ein früheres Softwarepaket kann eine bekannte Schwachstelle enthalten. Deshalb müssen Zielstand und Bedingungen des Rollbacks vorab geprüft werden.

Die Datenfrage bleibt ebenfalls bestehen. Werden Nutzungsrechte widerrufen oder Datenbestände als fehlerhaft erkannt, kann eine bloße Dateilöschung unzureichend sein, wenn daraus bereits Modelle entstanden sind. Welche Folgen rechtlich und technisch erforderlich sind, hängt vom Fall ab. Der Leitfaden verspricht keine universelle Möglichkeit, den Einfluss einzelner Daten nachträglich zuverlässig aus jedem Modell zu entfernen. Er empfiehlt, solche Abhängigkeiten durch Herkunfts- und Trainingsregister überhaupt erst nachvollziehbar zu machen.

12. Ein Incident-Verfahren, das physische und digitale Folgen verbindet

Bei einem Vorfall haben unmittelbarer Personenschutz und der freigegebene sichere Zustand Vorrang. Danach werden Beweise so gesichert, dass Diagnose und rechtliche Prüfung möglich bleiben. Ein unkontrollierter Neustart kann relevante Zustände überschreiben. Gleichzeitig darf Beweissicherung keine zusätzliche Gefahr erzeugen; die zuständige Betriebs- und Sicherheitsorganisation legt das Verfahren fest.

Der Bericht dokumentiert Zeitpunkt, betroffene Konfigurationen, Aufgaben, Datenflüsse, beobachtete Wirkung und bereits ergriffene Maßnahmen. Er trennt gesicherte Beobachtung von Hypothese. „KI-Fehler“ ist keine ausreichende Ursachenanalyse. Möglich sind fehlerhafte Eingaben, Modellgrenzen, falsche Konfiguration, Schnittstellenprobleme, Hardwaredefekte oder organisatorische Fehlannahmen.

Für Wiederinbetriebnahme werden Korrektur, Nachweis und Freigabe getrennt dokumentiert. Eine gefundene plausible Ursache ist noch kein Beweis ihrer vollständigen Beseitigung. Die Prüfung muss auch betrachten, ob weitere Roboter oder Standorte denselben Fehlerzustand besitzen. Bei Flotten können gemeinsame Komponenten oder Updates eine gemeinsame Ursache erzeugen.

13. Vertragliche Gestaltung: prüfbare Inhalte statt Musterklauseln

Das Paket liefert bewusst keine vermeintlich universellen Vertragsklauseln. Es benennt die Regelungsgegenstände: Leistungsumfang, Abnahme, Datenzugang, Nutzungszwecke, Rechte an Ergebnissen, Fernzugriff, Support, Sicherheitsmeldungen, Änderungen, Export, Löschung, Auditmöglichkeiten und Beendigung. Jede Klausel muss mit der tatsächlichen Architektur und dem anwendbaren Recht zusammenpassen.

Ein Datenvertrag sollte beispielsweise nicht nur eine Empfängerliste enthalten, sondern Zweck und Berechtigung jedes Empfängers. Eine Updatevereinbarung sollte nicht lediglich automatische Installation erlauben, sondern Transparenz, Freigabegrenzen und betriebliche Unterbrechungen regeln. Eine Servicezusage sollte unterscheiden, ob der Anbieter lediglich diagnostiziert oder einen produktiven Wiederanlauf schuldet.

Die technische Umsetzung wird gegen die Vereinbarung geprüft. Ein vertraglich untersagter Trainingszugriff ist unzureichend abgesichert, wenn Produktionsdaten in denselben unkontrollierten Speicher gelangen wie Forschungsdaten. Umgekehrt darf eine technische Sperre berechnete Zugangsansprüche nicht ohne geeignete Prüfung vereiteln. Recht und Architektur müssen dieselbe Wirklichkeit beschreiben.

14. Abnahme einer Daten- und Änderungsarchitektur

Vor Freigabe sollten Dateninventar, Rollenprüfung, Zweck- und Rechteübersicht, technische Zugriffskontrollen, Support- und Incident-Verfahren sowie Änderungsmanifest vorliegen. Die Prüfer kontrollieren nicht nur, ob Dokumente existieren, sondern ob ein konkreter Datenstrom und ein konkretes Update lückenlos durch diese Unterlagen verfolgt werden können.

Ein sinnvoller Testfall wählt eine Störungsaufnahme aus dem Betrieb. Das Team muss zeigen können, warum sie erhoben wurde, wer sie sehen darf, ob sie für Training geeignet und erlaubt ist, in welchem Modellstand sie verwendet wurde und welche Nachweise dessen Ausrollung tragen. Gelingt dieser Pfad nicht, liegt ein konkreter Governance- oder Dokumentationsengpass vor. Es ist dann präziser, diesen Engpass zu beheben, als pauschal mehr „KI-Compliance“ zu verlangen.

Prüffrage zum Abschluss: Sind unsere tatsächlichen Daten- und Änderungswege mit den dokumentierten Zwecken, Rechten, Pflichten und Sicherheitsannahmen deckungsgleich?

<!-- BEGIN AUTO-BIBLIOGRAPHY -->

Quellen zu diesem Dokument

Stabile Kennungen und genaue Fundstellen bleiben bei der PDF-Erstellung erhalten. Die genannten Quellen sind nicht sämtlich offline im Paket enthalten. Zugriffsgrenzen und Einschränkungen sind Teil des Nachweises.

Q014 · RoX-Konsortium

automatica 2025: ecosystem demonstrations. Stand/Publication: 2025. Zugriff: 2026-09-25. **Original:**

<https://www.project-rox.ai/en/automatica-2025/> **Fundstelle:** AI ecosystem and model retraining; Traceability and data control **Aussagebezug:** Demonstratorlogik für Datenaustausch und Modellverbesserung. **Zugriff:** Relevanter Inhalt online eingesehen **Grenze:** Demonstration und Zielbeschreibung, nicht Beweis einer flächendeckend produktiven Infrastruktur.

Q017 · Boston Dynamics

Stretch Privacy Notice. Stand/Publication: o. D.; Webseitenstand am Abrufdatum. Zugriff: 2026-09-25. **Original:**

<https://bostondynamics.com/products/stretch/privacy-notice/> **Fundstelle:** Service Logs; Performance Metrics; purposes of processing **Aussagebezug:** Beispiel ausdrücklich beschriebener Betriebs- und Diagnosedatenströme. **Zugriff:** Relevanter Inhalt online eingesehen **Grenze:** Herstellererklärung; kein Nachweis vollständiger Rechtskonformität eines konkreten Kundeneinsatzes.

Q022 · NIST

SP 800-82 Revision 3: Guide to Operational Technology (OT) Security. Stand/Publication: September 2023. Zugriff: 2026-09-25. **Original:** <https://csrc.nist.gov/pubs/sp/800/82/r3/final> **Fundstelle:** OT characteristics; risk management; architecture and safeguards **Aussagebezug:** Verfügbarkeit, physische Prozesse und

Sicherheitsanforderungen gemeinsam betrachten. **Zugriff:** Relevanter Inhalt online eingesehen **Grenze:** US-amerikanische technische Empfehlung, kein unmittelbar verbindliches EU-Recht.

Q023 · NIST

SP 800-218: Secure Software Development Framework (SSDF), Version 1.1. Stand/Publication: Februar 2022. Zugriff: 2026-09-25. **Original:** <https://csrc.nist.gov/pubs/sp/800/218/final> **Fundstelle:** Practice groups PO, PS, PW, RV **Aussagebezug:** Sichere Entwicklung, Releases und Schwachstellenbehandlung. **Zugriff:** Relevanter Inhalt online eingesehen **Grenze:** Bewusst feste Referenzversion; keine Behauptung, dies sei die jüngste aller Entwurfsfassungen.

Q026 · Europäische Kommission / DG CONNECT

AI Act – Regulatory framework for AI. Stand/Publication: Seitenstand 03.08.2026. Zugriff: 2026-09-25. **Original:** <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai> **Fundstelle:** Application timeline; AI Omnibus; integration with sectoral legislation **Aussagebezug:** Aktuelle Erläuterung der AI-Act-Zeitachse und sektoralen Umsetzung. **Zugriff:** Relevanter Inhalt online eingesehen **Grenze:** Kommissionserklärung ersetzt keine individuelle Systemklassifikation.

Q027 · Europäisches Parlament und Rat

Verordnung (EU) 2026/1744 zur Änderung des AI Act und sektoraler Rechtsakte. Stand/Publication: 08.07.2026; ABl. 24.07.2026. Zugriff: 2026-09-25. **Original:** <https://eur-lex.europa.eu/eli/reg/2026/1744/oj/eng> **Geprüfter Spiegelzugang:** <https://www.avvocati.prato.it/wp-content/uploads/2026/07/Digital-Omnibus-.pdf> **Fundstelle:** Art. 1 Nr. 2 (AI-Act-Art. 2 Abs. 2), Nr. 40 (Art. 113), Nr. 41 (Anhang I); Art. 3 (Maschinenverordnung Art. 8, 20, 47); Amtsblattseiten 15–16, 36–37, 40–41 **Aussagebezug:** Geänderte Fristen und sektorale Einbindung der Maschinenverordnung in Anhang I Abschnitt B. **Zugriff:** Amtsblatt-Spiegel inhaltlich und auszugsweise visuell geprüft; offizieller Direktabruf blockiert **Grenze:** Original-EUR-Lex-Abruf technisch blockiert. Amtsblatttext über Spiegel der Rechtsanwaltskammer Prato gelesen und relevante Seiten visuell geprüft; verbindlichen Originalstand vor Rechtsfreigabe sichern.

Q028 · Europäische Kommission / DG GROW

Machinery. Stand/Publication: o. D.; Webseitenstand am Abrufdatum. Zugriff: 2026-09-25. **Original:** https://single-market-economy.ec.europa.eu/sectors/mechanical-engineering/machinery_en **Fundstelle:** New Machinery Regulation / application date **Aussagebezug:** Maschinenverordnung (EU) 2023/1230, allgemeiner Anwendungsbeginn 20.01.2027. **Zugriff:** Relevanter Inhalt online eingesehen **Grenze:** Produktbezogene Pflichten, Übergang und Konformitätsverfahren einzelfallbezogen bestimmen.

Q029 · Europäische Kommission / DG CONNECT

Data Act explained. Stand/Publication: o. D.; Webseitenstand am Abrufdatum. Zugriff: 2026-09-25. **Original:** <https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained> **Fundstelle:** Chapter II: connected products / data access; users and data holders; application **Aussagebezug:** Datenzugang bei vernetzten Produkten, Rollen, Roh-/vorverarbeitete Daten und Grenzen. **Zugriff:** Relevanter Inhalt online eingesehen **Grenze:** Erklärung; keine Eigentumszuteilung und keine pauschale datenschutzrechtliche Trainingserlaubnis.

Q030 · Europäisches Parlament und Rat

Verordnung (EU) 2023/2854 – Data Act. Stand/Publication: 13.12.2023. Zugriff: 2026-09-25. **Original:** <https://eur-lex.europa.eu/eli/reg/2023/2854/oj> **Fundstelle:** Art. 2–6, 8–13 und 50; insbesondere Art. 3 Abs. 1 und zeitliche Anwendung **Aussagebezug:** Juristische Fundstellen zu Rollen, Zugang, Nutzung, Weitergabe und Gestaltungspflichten. **Zugriff:** Originalfundstelle dokumentiert; Direktabruf blockiert; inhaltlicher Abgleich über amtliche Erläuterung Q029 **Grenze:** Original-Direktabruf in dieser Runde blockiert; Aussagen werden zusätzlich auf Q029 gestützt. Für Vertragsfreigabe konsolidierten Originaltext beziehen.

Q031 · Europäische Kommission / DG CONNECT

Cyber Resilience Act – Reporting obligations. Stand/Publication: Seitenstand 11.09.2026. Zugriff: 2026-09-25. **Original:** <https://digital-strategy.ec.europa.eu/en/policies/cra-reporting> **Fundstelle:** What are the main rules?;

Where should manufacturers submit? **Aussagebezug:** Herstellermeldungen ab 11.09.2026; 24-/72-Stundenstufen; differenzierte Abschlussfristen; ENISA-SRP. **Zugriff:** Relevanter Inhalt online eingesehen **Grenze:** Rollen und Meldeereignisse müssen zutreffen; keine pauschale Pflicht jedes Betreibers für jede Störung.

Q032 · Europäische Kommission / DG CONNECT

Cyber Resilience Act – Summary of the legislative text. Stand/Publication: o. D.; Webseitenstand am Abrufdatum. Zugriff: 2026-09-25. **Original:** <https://digital-strategy.ec.europa.eu/en/policies/cra-summary> **Fundstelle:** Chapter I (scope); Chapter II (manufacturer obligations); final provisions **Aussagebezug:** Produktbezug, Lebenszyklus, technische Dokumentation und Konformitätsarchitektur. **Zugriff:** Relevanter Inhalt online eingesehen **Grenze:** Ausnahmen und konkrete Pflichten sind am Rechtsakt und der einschlägigen Fassung zu bestimmen.

Q033 · Europäisches Parlament und Rat

Verordnung (EU) 2024/2847 – Cyber Resilience Act. Stand/Publication: 23.10.2024. Zugriff: 2026-09-25. **Original:** <https://eur-lex.europa.eu/eli/reg/2024/2847/oj> **Fundstelle:** Art. 2 (Anwendungsbereich), 13 (Hersteller), 14 (Meldungen), 71 (Anwendung), Anhang I **Aussagebezug:** Primäre juristische Fundstelle der CRA-Lebenszyklusplichten. **Zugriff:** Originalfundstelle dokumentiert; Direktabruf blockiert; Erläuterungen Q031/Q032 geprüft **Grenze:** Original-Direktabruf blockiert; tragende Aussagen gegen Q031/Q032 geprüft. Support- und Ausnahmeprüfung braucht konkreten Originalabgleich.

Q034 · Europäischer Datenschutzausschuss

Guidelines 07/2020 on the concepts of controller and processor in the GDPR, version 2.0. Stand/Publication: 07.07.2021. Zugriff: 2026-09-25. **Original:** https://www.edpb.europa.eu/documents/guideline/guidelines-072020-on-the-concepts-of-controller-and-processor-in-the-gdpr_en **Geprüfter Spiegelzugang:** https://www.edpb.europa.eu/system/files/documents/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf **Fundstelle:** Teil I: controller, joint controller, processor; Teil II: consequences and contractual arrangements **Aussagebezug:** Rollen richten sich nach tatsächlichen Zwecken und Mitteln, nicht nur Vertragsüberschrift. **Zugriff:** Relevanter Inhalt online eingesehen **Grenze:** Leitlinie, keine individuelle Behördenentscheidung.

Q035 · Europäisches Parlament und Rat

Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung. Stand/Publication: 27.04.2016. Zugriff: 2026-09-25. **Original:** <https://eur-lex.europa.eu/eli/reg/2016/679/oj> **Fundstelle:** Art. 5, 6, 9, 13/14, 25, 28, 30, 32–35, 44 ff. **Aussagebezug:** Prüfroute für personenbezogene Roboterdaten, Sicherheit, Rollen und Transfers. **Zugriff:** Originalfundstelle dokumentiert; Direktabruf blockiert; Rollenleitlinie Q034 inhaltlich geprüft **Grenze:** Original-Direktabruf blockiert. Rollenprüfung auf Q034 gestützt; individuelle Rechtsgrundlage, Gesundheitsdaten und Beschäftigtenrecht gesondert prüfen.

Q037 · Medical Device Coordination Group (MDCG)

MDCG 2019-11 rev.1 – Guidance on Qualification and Classification of Software under MDR and IVDR. Stand/Publication: Juni 2025, rev.1. Zugriff: 2026-09-25. **Original:** https://health.ec.europa.eu/document/download/b45335c5-1679-4c71-a91c-fc7a4d37f12b_en?filename=mdcg_2019_11_en.pdf **Fundstelle:** Abschnitte 1–3 (S. 4–15), 7 (Module), 8 (Änderungen), Anhang I; S. 7–9 besonders zur Zweckbestimmung **Aussagebezug:** Softwarequalifikation hängt an medizinischer Zweckbestimmung; nicht jede Software im Krankenhaus ist Medizinprodukt. **Zugriff:** Relevanter Inhalt online eingesehen **Grenze:** Nicht rechtsverbindliche MDCG-Leitlinie; keine vollständige Klassifikation robotischer Hardware oder Zubehörteile.

Q039 · Bundesministerium der Justiz / Gesetze im Internet

Betriebssicherheitsverordnung – § 3 Gefährdungsbeurteilung. Stand/Publication: o. D.; Webseitenstand am Abrufdatum. Zugriff: 2026-09-25. **Original:** https://www.gesetze-im-internet.de/betrsv_2015/_3.html **Fundstelle:** Abs. 1–4, 6–8 **Aussagebezug:** Arbeitgeberpflicht, CE-Abgrenzung, Einbeziehung von Arbeitsumgebung und Störungen, fachkundige Beurteilung, Prüfungen und Aktualisierung. **Zugriff:** Offizieller Einzelnormtext online vollständig eingesehen **Grenze:** Anwendbarkeit weiterer Vorschriften und konkrete Schutzmaßnahmen fachkundig bestimmen.

Q040 · Europäische Kommission / DG CONNECT

Cyber Resilience Act – Manufacturers. Stand/Publication: Seitenstand 14.08.2026. Zugriff: 2026-09-25. **Original:** <https://digital-strategy.ec.europa.eu/en/policies/cra-manufacturers> **Fundstelle:** Before / At / After placing on the market **Aussagebezug:** Risikobeurteilung, Dokumentation, Supportangabe und Schwachstellenbehandlung im Produktlebenszyklus. **Zugriff:** Relevanter Inhalt online eingesehen **Grenze:** Pflichten gelten abhängig von Produkt, Rolle und zeitlicher Anwendung; keine konkrete Konformitätsprüfung.

Q041 · Autoriteit Consument & Markt (ACM), Niederlande

Data Sharing Guidelines – preliminary version. Stand/Publication: Vorläufige Fassung, Abruf 25.09.2026. Zugriff: 2026-09-25. **Original:** <https://www.acm.nl/system/files/documents/data-sharing-guidelines.pdf> **Fundstelle:** Abschnitt 2.3, Rn. 32–33 (S. 13); 2.4 (Rollen); 4 (Zugang); 5 (Nutzungsbedingungen) **Aussagebezug:** Ergänzende Aufsichtsorientierung zu Zugangsgestaltung, Rollen und Datenweitergabe. **Zugriff:** Relevanter Inhalt online eingesehen **Grenze:** Ausdrücklich vorläufige Leitlinie; niederländische Zuständigkeitsangaben nicht auf Deutschland übertragen. Englische Formulierung entered into force für September 2025 wird hier nicht übernommen: maßgeblich ist der Anwendungsbeginn.

Q042 · Europäische Kommission / DG CONNECT

Cyber Resilience Act – Overview. Stand/Publication: Seitenstand 07.09.2026. Zugriff: 2026-09-25. **Original:** <https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act> **Fundstelle:** Application timeline **Aussagebezug:** Allgemeine CRA-Pflichten ab 11.12.2027, Herstellermeldungen ab 11.09.2026. **Zugriff:** Relevanter Inhalt online eingesehen **Grenze:** Zeitachse allein entscheidet weder Produktklassifikation noch individuelle Pflicht.

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.