

IMPULSPAPIER

Fachliche Anregung – kein Normentwurf

HU-RAC

Ein Denkmodell zur Klassifikation smarter Robotiksysteme nach Datenhoheit und Datensicherheit

*Ein Beitrag zur öffentlichen Diskussion über eine mögliche zukünftige Normungs- und
Regulierungssystematik*

*Fragen der technischen und funktionalen Sicherheit werden ausdrücklich ausgeklammert und in
einem angekündigten zweiten Impulspapier gesondert behandelt.*

Version 0.3.1

Stand: April 2026

Autorin: Humanide GmbH

*Dieses Dokument ist kein Normentwurf und kein Standard.
Es stellt keine verbindliche Anforderung dar und begründet keine Rechts- oder Leistungspflichten.*

Es dient ausschließlich der fachlichen Anregung.

Rechtlicher Hinweis

Dieses Impulspapier ist eine unverbindliche fachliche Darstellung zu Diskussionszwecken. Es handelt sich weder um einen Normentwurf im Sinne des DIN- oder ISO-Verfahrens noch um eine abgestimmte Konsortialposition, einen Standard, eine technische Regel oder eine Empfehlung im Sinne des § 823 BGB. Die darin enthaltenen Einstufungen, Kategorien, Matrizen und Formulierungen sind ausschließlich als Anregung zur weiteren Diskussion unter interessierten Kreisen gedacht.

Die Autorin schließt jegliche Haftung für Entscheidungen aus, die aufgrund der in diesem Dokument enthaltenen Darstellungen getroffen werden. Eine Verwendung dieses Dokuments oder einzelner Teile davon in Ausschreibungen, Verträgen, behördlichen Verfahren oder rechtsverbindlichen Kontexten ist nicht vorgesehen und erfolgt gegebenenfalls auf alleinige Verantwortung der verwendenden Stelle.

Die rechtsbezogenen Formulierungen zu Datenschutz-Grundverordnung (DSGVO), KI-Verordnung, Maschinenverordnung, Cyber Resilience Act und weiteren Rechtsakten sind fachlich eingeordnet, jedoch nicht anwaltlich geprüft und ersetzen keine individuelle Rechtsberatung.

Die Bezeichnung HU-RAC ist im Rahmen dieses Papiers als Arbeitsbegriff gewählt. Die im Papier referenzierten RARI-Daten stammen aus der Keynote von N. Radford (Persona AI) auf dem Humanoids Summit 2025 (11.12.2025, Mountain View) und werden hier als Sekundärquelle zitiert. Marken- und Urheberrechte an Bezeichnungen und Darstellungen Dritter bleiben bei den jeweiligen Rechtsinhabern.

Nutzung und Weitergabe

Die Weitergabe und Zitation dieses Impulspapiers ist ausdrücklich erwünscht, sofern die Urheberschaft der Humanide GmbH benannt und der Charakter als unverbindliches Diskussionsdokument erkennbar bleibt. Auszüge dürfen unter Angabe der Quelle verwendet werden.

Zusammenfassung in drei Absätzen

Ein Mähroboter im Garten und ein humanoider Pflege-Companion im Schlafzimmer einer Demenzkranken sollten in Fragen von Datenhoheit und Datensicherheit nicht nach derselben Logik bewertet werden. Heute werden sie es – mal implizit, mal ausdrücklich. Dieses Papier schlägt vor, smarte Robotersysteme entlang von sechs Kontextdimensionen in fünf Kategorien (HU-RAC 1 bis HU-RAC 5) einzuordnen und jeder Kategorie ein abgestuftes Erwartungsprofil in den Fragen von Datenschutz, Schlüsselhoheit, Mandantentrennung, KI-Bezug und Betriebskontinuität zuzuordnen. Der Ansatz folgt dem Prinzip der stärksten Belastung: Die höchste Einstufung auf einer einzelnen Achse bestimmt die Gesamtkategorie.

HU-RAC ist dabei nicht als Ersatz bestehender Rechtsakte gedacht, sondern als Overlay: ein domänenspezifisches Ordnungs- und Übersetzungsraster, das DSGVO, KI-Verordnung, Maschinenverordnung, Cyber Resilience Act und die einschlägigen ISO-Normen kontextabhängig anwendbar macht. Die Regelwerke existieren; was fehlt, ist ihre kohärente, roboterspezifische Operationalisierung.

Drei jüngere Ereignisse zeigen, dass die Lücke nicht hypothetisch ist: Im Februar 2026 entdeckten Sicherheitsforscher einen Autorisierungsfehler im Backend eines marktführenden Herstellers autonomer Haushaltsroboter, der Fremdzugriff auf tausende Geräte erlaubte. Im Februar 2025 zog ein marktbestimmender US-amerikanischer Technologiekonzern seine Zero-Knowledge-Cloud-Schutzfunktion für britische Nutzer zurück, nachdem britische Sicherheitsbehörden eine entsprechende Anordnung erließen. Und 2024 meldete ein europäischer Hersteller vernetzter Blutdruckmessgeräte Insolvenz an – mit der Abschaltung der Cloud-Infrastruktur verschwanden nicht nur die Apps, ohne die die Geräte funktionslos waren, sondern auch die historischen Gesundheitsdaten der Nutzer. Für humanoide Serviceroboter in sensiblen Umgebungen sind das keine Randnotizen – sie berühren den Kern der Vertrauensfrage.

Das Denkmodell integriert einen zweiten Blick: den kommerziellen. Das RARI-Framework von Persona AI (Radford, Humanoids Summit 2025) bewertet Branchen nach ihrer Adoptionsreife – und zeigt, dass gerade die regulatorisch komplexen Branchen (Healthcare, Home) die niedrigste kommerzielle Reife aufweisen. Eine klare Klassifikationssystematik senkt nicht nur Compliance-Reibung, sondern erhöht die Adoptionsreife genau dort, wo der Markt heute ins Stocken gerät. Normung wird in dieser Lesart zum Marktoffnungs-Hebel.

Eine wichtige Einschränkung vorneweg: Dieses Papier behandelt ausdrücklich nicht die Fragen der technischen und funktionalen Sicherheit. Das Notaus-Problem bei dynamisch stabilen humanoiden Systemen, das Stromausfallverhalten, die Power-and-Force-Limiting-Grenzwerte im nicht-industriellen Kontext – all das verdient ein eigenes Impulspapier, das die Humanide GmbH gesondert vorbereitet. Kapitel 2 macht diese Abgrenzung explizit.

1 Warum dieses Papier

Smarte Robotiksysteme durchdringen Arbeitswelt und Alltag in einer Geschwindigkeit, für die das geltende Regulierungs- und Normengefüge nicht gebaut wurde. Die Maschinenverordnung behandelt Mähroboter und humanoide Pflege-Begleiter weitgehend unter demselben Dach. Die KI-Verordnung kennt zwar Hochrisiko-Kategorien, aber keine Feinabstufung, die der Heterogenität der Robotik gerecht würde. Die Produkthaftungsrichtlinie bleibt in ihrer Risikologik ebenso grob. Das Ergebnis ist eine doppelte Fehlanpassung: Consumer-Produkte werden tendenziell überreguliert, Hochrisiko-Einsätze werden tendenziell unterreguliert. Beides ist dem Markt abträglich.

Drei Ereignisse aus den letzten 18 Monaten haben gezeigt, wie konkret diese Lücke wird, sobald Serviceroboter in sensible Bereiche vordringen.

1.1 Drei Episoden, die nachdenklich machen sollten

Ein Backend-Vorfall bei einem Consumer-Robotik-Hersteller, Februar 2026

Im Februar 2026 entdeckten Sicherheitsforscher einen Autorisierungsfehler im MQTT-Backend eines marktführenden Herstellers autonomer Haushaltsroboter. Rund 6.700 Geräte wurden kompromittiert. Angreifer mit gültigen Nutzer-Zugangsdaten konnten durch Manipulation der Geräte-Referenzen auf Kameras, Mikrofone und Grundrisse von Wohnungen zugreifen, die anderen Nutzern gehörten. Die Transportverschlüsselung war einwandfrei. Die Schwachstelle lag nicht in der Kryptografie, sondern in der Autorisierungslogik: Ein Multi-Tenant-Backend mit gemeinsamem Pool und Token-basierter Zuordnung ermöglichte Querschlüsse. Lektion: Transportverschlüsselung schützt nicht vor Fehlern in der Mandantentrennung.

Die Rücknahme einer Zero-Knowledge-Cloud-Funktion in Großbritannien, Februar 2025

Ein marktbestimmender US-amerikanischer Technologiekonzern hatte seit 2023 eine Zero-Knowledge-Architektur für Cloud-Speicherdienste angeboten: Die kryptografischen Schlüssel lagen beim Nutzer, der Anbieter konnte technisch nicht auf die Klartextdaten zugreifen. Im Februar 2025 zog der Konzern diese Funktion für britische Nutzer zurück, nachdem die britischen Sicherheitsbehörden unter dem dortigen Rechtsrahmen für nachrichtendienstliche Befugnisse eine entsprechende Anordnung erließen. Lektion: Nur was der Anbieter technisch nie besessen hat, kann er staatlichen Stellen auch unter Zwang nicht übergeben. Vergleichbare Rechtsgrundlagen existieren in Deutschland (G10-Gesetz, TKÜV), Frankreich und auf EU-Ebene in Diskussion.

Die Insolvenz eines cloudabhängigen Medizingeräte-Herstellers, 2024

Ein europäischer Hersteller vernetzter Blutdruckmessgeräte meldete im Jahr 2024 Insolvenz an, schaltete seine Cloud-Infrastruktur ab – und mit ihr die Apps, ohne die die Geräte funktionslos waren, sowie die historischen Messdaten seiner Nutzer, die nicht lokal verfügbar waren. Es ist ein Muster, das sich bei mehreren Smart-Home- und Connected-Health-Anbietern wiederholt hat. Für ein Gesundheits- oder Pflege-Setting mit humanoidem Assistenzsystem wäre ein solcher Ausfall existenzieller. Lektion: Cloudabhängigkeit ohne architektonischen und vertraglichen Kontinuitätsschutz erzeugt ein Risiko, das mit dem Pflege- und Medizinkontext schwer vereinbar ist.

1.2 Die Leitfrage

Wie kommt man zu einer abgestuften Bewertung, die einem Pool-Reinigungsroboter in Fragen der Datenhoheit nicht die Last eines OP-Assistenzsystems aufbürdet, und umgekehrt einem Pflege-Companion nicht die Regulierungstiefe eines Saugroboters

zugesteht? Und zwar so, dass die Abstufung nicht willkürlich wirkt, sondern an klaren Kontextdimensionen entlang denkbar ist, die sich in die bestehende Regulierungslandschaft einfügen? Dieses Papier macht einen Vorschlag – begrenzt auf die Fragen von Datenhoheit und Datensicherheit, als Overlay auf bestehendes Recht. Warum diese doppelte Begrenzung – thematisch und im Verhältnis zu bestehenden Regelwerken – nötig und sinnvoll ist, machen die folgenden Kapitel explizit.

2 Was dieses Papier behandelt – und was nicht

2.1 Der Betrachtungsrahmen

Dieses Impulspapier befasst sich mit zwei verbundenen Themenfeldern: **Datenhoheit** (Kontrolle über die im Betrieb smarter Robotersysteme anfallenden Daten, einschließlich Speicherort, Schlüsselverwaltung, Mandantentrennung und staatlicher Zugriffsschutz) und **Datensicherheit** (Schutz dieser Daten vor unbefugtem Zugriff, Integritätsverlust und Indiensthaltungs-Unterbrechung). Innerhalb dieses Rahmens betrachtet es auch die unmittelbar angrenzenden Felder: die regulatorische Einordnung nach DSGVO und KI-Verordnung, den Betroffenenenschutz im Sinne der Datenschutz-Grundrechte, und die Betriebskontinuität als Voraussetzung dafür, dass Daten auch bei Anbieter-Insolvenz nicht verloren gehen.

2.2 Außerhalb des Rahmens: die technische und funktionale Sicherheit

Das Papier behandelt bewusst nicht die Fragen der technischen und funktionalen Sicherheit. Diese verdienen ein eigenes Denkmodell mit eigener Fachkultur, eigenen Normungsbezügen und eigenem Beteiligtenkreis (Berufsgenossenschaften, Prüfstellen, Maschinenbau-Fachgremien, Luftfahrt-Behörden). Die Vermischung beider Themenfelder in einem einzigen Papier würde beiden nicht gerecht.

Konkret sind folgende Fragen aus dem Betrachtungsrahmen dieses Papiers ausgenommen:

- Notaus-Logik und Abschaltkonzepte bei dynamisch stabilen und flugfähigen Systemen
- Verhalten bei Stromausfall bei bipedalen Humanoiden und Quadrupeden
- Power-and-Force-Limiting-Grenzwerte im nicht-industriellen Kontext
- Dynamische Stabilität, Sturzverhalten und Absturzrisiken
- Aerospace-Kreuzungsfragen (UAS, Luftfahrt-Zulassungen) in Verbindung mit der Maschinenverordnung
- Zertifizierbarkeit lernender KI-Komponenten als Sicherheitsfunktion nach ISO 13849-1
- Zulassungs- und Baumusterprüfungsfragen durch benannte Stellen

2.3 Ein konkretes Beispiel für den Klärungsbedarf: der Notaus-Konflikt

Warum diese Fragen nicht nebenbei in ein Datenhoheits-Papier hineingeschrieben werden können, zeigt ein einziges Beispiel besonders deutlich: das Notaus-Problem bei humanoiden Robotern.

Die bestehende Maschinensicherheitsnormung – insbesondere ISO 13850 – geht von einer einfachen Grundannahme aus: Das energetisch abgeschaltete System ist der sichere Zustand. Bei stationären Industrierobotern, bei radbasierten Cobots und bei den meisten klassischen Maschinen stimmt das. Bei einem bipedalen humanoiden Roboter stimmt es nicht. Wer einem laufenden Humanoiden per Notaus die Aktorik abschaltet, provoziert einen unkontrollierten Fall – mit Schaden an Personen in der Umgebung, am Gerät selbst und möglicherweise an empfindlichen Objekten. Bei einem flugfähigen System ist das Problem noch drastischer: Ein Multikopter bei Notaus fällt vom Himmel. Ein Flugzeug hat aus gutem Grund keinen Notaus-Knopf im Cockpit.

Die naheliegende Alternative wäre, humanoide Roboter in der EU so einzuhegen, wie klassische Industrieroboter eingehengt werden: physisch abgegrenzt, in einem Schutzkäfig, mit Sicherheitslichtschranken. Genau das ist jedoch funktional absurd. Ein Pflege-Companion im Käfig hat keinen Zweck. Ein haushaltsnaher Assistenzroboter auch nicht. Ein

Kochroboter in der Gastronomie oder ein Lieferroboter im öffentlichen Raum ebenfalls nicht. Die Daseinsberechtigung dieser Systeme hängt gerade an ihrer Fähigkeit, sich in menschlichen Umgebungen ungekäftigt zu bewegen.

Zwischen "Notaus mit Kollaps" und "Einhegung im Käfig" liegt der eigentliche Lösungsraum – und er ist normungstechnisch weitgehend offen. Denkbare Ansätze reichen von graceful degradation (kontrolliertes Hinsetzen oder Abstützen) über adaptive Abschaltlogiken (je nach Bewegungszustand) bis zu redundanten Fallback-Systemen (vergleichbar der Luftfahrt-Praxis). Die ISO 25785-1 für dynamisch stabile Systeme ist im Working-Draft-Stadium und wird diese Fragen mindestens teilweise adressieren, aber der Zeitpunkt ihrer Veröffentlichung ist offen.

2.4 Dringlichkeit: Warum ein zweites Impulspapier folgen muss

Die Maschinenverordnung (EU) 2023/1230 wird ab dem 20. Januar 2027 verbindlich – ohne Übergangsfrist. Humanoide und dynamisch stabile Systeme sind eindeutig von ihr erfasst. Wenn bis dahin keine tragfähige Antwort auf die Notaus-Frage und verwandte Probleme entwickelt ist, bleiben Anbietern und Betreibern in der EU im Wesentlichen drei unattraktive Wege: die riskante Umsetzung klassischer Notaus-Logik mit bekannten Nebenwirkungen, die faktische Einhegung der Systeme in nutzlose Käfige, oder der Rückzug aus dem europäischen Markt. Keiner dieser Wege dient dem Ziel, humanoide Servicerobotik in Europa zum Erfolg zu führen.

Die Humanide GmbH kündigt deshalb an, **ein zweites Impulspapier** zu den Fragen der technischen und funktionalen Sicherheit smarter Robotiksysteme vorzubereiten. Der geplante Fokus liegt auf:

- Abschaltlogiken bei dynamisch stabilen und flugfähigen Systemen (graceful degradation, kontrolliertes Hinsetzen, Fallback-Redundanz)
- Abgrenzung zur klassischen Notaus-Konzeption nach ISO 13850
- Diskussion der Zertifizierbarkeit lernender Sicherheitsfunktionen
- Power-and-Force-Limiting-Grenzwerte im Pflege- und Haushaltskontext
- Schnittstellen zur Luftfahrt-Zulassung bei UAS und flugfähigen Robotern

Das zweite Papier wird eigenständig, mit eigenem Beteiligtenkreis und eigener Diskussionsarchitektur erarbeitet. Die beiden Impulspapiere werden sich jedoch kreuzweise referenzieren – denn in der praktischen Anwendung gehören Datenhoheit und technische Sicherheit zusammen, auch wenn sie in der Problemanalyse getrennt behandelt werden müssen.

Bis dahin verweist dieses Papier in den einschlägigen Kapiteln auf die jeweils geltenden oder in Entwicklung befindlichen Maschinensicherheitsnormen, ohne eigene Erwartungen in diesem Feld zu formulieren. Wo die Matrizen in Kapitel 5 auf Maschinensicherheitsaspekte angrenzen, ist das ausdrücklich als offener Randpunkt zu verstehen.

3 Vier Leitideen des Denkmodells

3.1 Leitidee 1 – Nicht die Bauart, sondern das Zusammenspiel von Achsen entscheidet

Ein humanoider Bauform-Roboter ist nicht per se sensibler als ein stationärer Industrieroboter. Ein Mähroboter mit integrierter Kamera und Cloud-Anbindung kann in der Datendimension mehr Sensibilität tragen als ein biped laufender Serviceroboter ohne Personenerkennung. Deshalb schlägt das Modell sechs Betrachtungsachsen vor, die je einzeln bewertet werden. Die Gesamteinstufung folgt dem Prinzip der stärksten Belastung: Der höchste Wert auf einer beliebigen Achse bestimmt die Kategorie. Das verhindert, dass eine einzelne Hochrisiko-Dimension durch niedrige Werte auf anderen Achsen ausgemittelt wird.

3.2 Leitidee 2 – Fünf Stufen reichen, mehr schadet

Ein zu feingranulares Modell wird in der Praxis nicht angewendet. Fünf Kategorien (HU-RAC 1 bis 5) scheinen ein Kompromiss, der zwischen Consumer-Bagatellen und staatlich-sensitiven Anwendungen ausreichend differenziert, ohne operativ überfordernd zu wirken. Das Vorbild sind etablierte Stufenmodelle aus anderen Feldern: die Common Criteria Evaluation Assurance Levels, die Automotive SPICE Levels, die Performance Levels der ISO 13849-1. Fünf Stufen sind in diesen Kontexten anwendbar und akzeptiert.

3.3 Leitidee 3 – Regulatorische und kommerzielle Betrachtung sind Spiegel

Die vorliegende Arbeit wurde angeregt durch die Begegnung mit dem RARI-Framework (Robot Adoption Readiness Index), vorgestellt von Nicolaus Radford (Persona AI) auf dem Humanoids Summit 2025 in Mountain View. RARI bewertet acht Anwendungsbranchen auf kommerzielle Adoptionsreife. Die Rangfolge reicht von Heavy Industry (Score 100) und Automotive (96,9) über Warehousing und Construction bis zu Home (nahe 0). Legt man diese Rangfolge über eine Klassifikation nach Datenhoheit und Datensicherheit, zeigt sich ein überraschendes Muster: Branchen mit hoher kommerzieller Reife liegen in einem schmalen mittleren regulatorischen Korridor. Branchen mit niedriger kommerzieller Reife (Healthcare, Home) streuen breit – von sehr niedrig bis sehr hoch. Die Unklarheit der datenschutzrechtlichen und datenhoheitsbezogenen Anforderungen ist Teil der Adoptionsreibung. Ein klares Klassifikationsmodell kann diese Reibung senken – und damit Markt freilegen, der heute blockiert ist.

3.4 Leitidee 4 – HU-RAC ist Overlay, nicht Ersatz

Es existiert bereits ein dichtes Geflecht einschlägiger Rechtsakte und Normen: DSGVO mit Art. 32 (Sicherheit), Art. 25 (Privacy by Design), Art. 28 (AVV), Art. 35 (DSFA); KI-Verordnung mit Hochrisiko-Pflichten zu Dokumentation, Logging, Transparenz und menschlicher Aufsicht; Maschinenverordnung; Produkthaftungsrichtlinie; Cyber Resilience Act; ISO 10218, ISO 13482, EN ISO 12100. Die Lücke liegt deshalb nicht bei fehlenden Regeln, sondern bei der fehlenden Kohärenz zwischen diesen Regelwerken und ihrer mangelnden Operationalisierung für die konkreten Einsatzszenarien smarterer Robotik.

HU-RAC positioniert sich explizit nicht als Ersatz dieser Rechtsakte und Normen, sondern als Overlay: ein domänenspezifisches Ordnungs- und Übersetzungsraster, das die bestehenden Regelwerke kontextabhängig anwendbar macht. Das Modell orchestriert, statt zu duplizieren. Annex E enthält ein Mapping-Schema, das diese Orchestrierung in vier Schritten nachvollziehbar macht: AI-Act-Einstufung, HU-RAC-Einstufung, DSGVO-Abgleich und Ableitung zusätzlicher HU-RAC-spezifischer Erwartungen. Diese Positionierung hat

auch Konsequenzen für die Erwartungsmatrix in Kapitel 5: Viele als essenziell markierte Punkte sind ohnehin rechtlich verpflichtend, andere gehen über den Marktstandard hinaus. Kapitel 5 macht diese Unterscheidung durch die Aufspaltung in E-Min und E-Plus sichtbar.

HU-RAC steht dabei in einem definierten Feld verwandter Klassifikationsansätze, hebt sich aber in der Zusammenstellung seiner Fokussierung von jedem bekannten System ab: Autonomie-Grading-Systeme wie SAE J3016 (Fahrzeuge), LASR (chirurgische Robotik) und die 2025/2026 veröffentlichten chinesischen Standards T/CIE 298-2025 und das MIIT-Standardsystem adressieren Fähigkeitsstufen und Entscheidungsautonomie, nicht Datenhoheit. Die CPST-Taxonomie von Ning und Ding (2026) adressiert die ontologische Frage, welche Art von Entität ein autonomes System ist, und leitet daraus Governance-Stufen bis hin zu Rechtspersönlichkeits-Fragen ab. Das Google Robotics Privacy Framework (2024) bleibt prinzipientreu (Identify, Assess, Enforce) ohne abgestufte Einstufungssystematik. HU-RAC verbindet als einziges Modell den Robotik-Einsatzkontext mit einem Datenhoheits-Fokus in einer Overlay-Logik auf europäisches Recht. Annex D.3 enthält eine Übersicht verwandter Klassifikationsansätze.

4 Das Denkmodell: HU-RAC in fünf Kategorien

4.1 Die sechs Betrachtungsachsen

Achse 1 – Einsatzumgebung

Die Umgebung, in der das System arbeitet, bestimmt Strukturiertheit, Publikumsexposition und rechtlichen Rahmen. Die Spannweite reicht von privater Outdoor-Nutzung über gewerblich-geschlossene und publikumsintensive Bereiche bis zu Pflege, Bildung, Kinderbetreuung und militärisch-sensitiven Kontexten.

Achse 2 – Bauart und Mobilität

Stationär, radbasiert mobil, flugfähig, bipedal oder dynamisch stabil, aquatisch. Jede Bauart triggert andere Maschinensicherheitsaspekte und andere Normungsbezüge.

Achse 3 – Datenkategorien

Von reiner Maschinentelemetrie über personenbeziehbare Umgebungsdaten und biometrische Daten bis zur intimen Langzeitbeobachtung (Alltag, Gespräche, Pflegesituationen). Die Datenkategorie entscheidet über die datenschutzrechtliche Schwere.

Achse 4 – KI-Risikoklasse

Eingeordnet an der KI-Verordnung: von Bagatellfunktionen über begrenztes Risiko und Hochrisiko bis zu Hochrisiko mit vulnerabler Zielgruppe oder staatlicher Sensitivität.

Achse 5 – Physisches Gefährdungspotenzial (als Kontextinformation)

Kinematische Energie, Reichweite, Interaktionsfähigkeit mit Menschen. Von Power-and-Force-Limiting-Klasse über Cobot-Niveau bis zu waffenfähig oder Dual-Use-sensitiv. Diese Achse dient hier ausschließlich als Kontextinformation zur Einstufung in eine HU-RAC-Kategorie; maschinensicherheitsrechtliche Erwartungen werden aus ihr in diesem Papier bewusst nicht abgeleitet (siehe Kapitel 2).

Achse 6 – Betroffenenkreis

Wer ist rechtlich und ethisch berührt? Nur Betreiber, Mitarbeitende, unbeteiligte Dritte, vulnerable Gruppen (Patienten, Kinder, Menschen mit Demenz), oder rechtlich besonders geschützte Kreise (Berufsheimnisträger).

4.2 Die Aggregationslogik

Das HU-RAC-Denkmodell schlägt vor, die Gesamtkategorie durch den höchsten Wert auf einer beliebigen der sechs Achsen zu bestimmen. Ein System, das auf fünf Achsen niedrig einzustufen wäre und auf einer Achse die höchste Stufe erreicht, würde als Tier-5-System gedacht. Diese Regel folgt dem Grundsatz der stärksten Belastung, analog zur Gefahrgut-Einstufungslogik und zur risikoorientierten Einstufungspraxis der Maschinenverordnung. Sie verhindert, dass eine einzelne kritische Dimension durch Mittelung verdeckt wird.

Ausnahme 1 – Technisch eingehegte temporäre Hochrisiko-Modi

Ein zeitlich oder funktional begrenzter Hochrisiko-Modus (etwa ein Diagnosemodus mit biometrischer Einmalerfassung) führt nicht automatisch zur Anhebung der Gesamtkategorie auf Tier 4 oder 5, sofern kumulativ folgende Bedingungen erfüllt sind:

- Der Modus ist nur mit expliziter Einwilligung der betroffenen Person oder durch autorisiertes Fachpersonal aktivierbar.

- Starke technische Schutzmaßnahmen sind aktiv (lokale Verarbeitung ohne Cloud-Anbindung, Air-Gap zur allgemeinen Telemetrie, sofortige Löschung nach Zweckerreichung).
- Jede Aktivierung wird protokolliert und ist auditierbar.
- Die funktionale Begrenzung ist in der technischen Dokumentation und in der Konformitätserklärung ausgewiesen.

Sind diese Bedingungen erfüllt, richtet sich die Einstufung nach dem Regelbetrieb. Andernfalls greift die Grundregel.

Ausnahme 2 – Forschungseinsätze

Bei reinen Forschungseinsätzen im Sinne von Art. 2 Abs. 6 AI Act und unter entsprechenden Schutzmaßnahmen (Ethikkommission, begrenzter Personenkreis, Anonymisierung, Art. 89 DSGVO) kann für die Dauer der Forschung ein um ein Tier niedrigeres Einstufungsregime angewandt werden, sofern dies in der DSFA explizit begründet ist.

Zweite Aggregationsregel – Mehrfach-Mittelbelastung

Um Unterklassifikation bei vielschichtigen Systemen zu verhindern, gilt ergänzend: Wenn drei oder mehr der sechs Achsen im mittleren Bereich liegen, wird mindestens HU-RAC 3 erreicht, auch wenn keine einzelne Achse die höchste Stufe erreicht. Damit werden komplexe Systeme mit breiter Mittelbelastung nicht als Consumer-Anwendung eingestuft.

4.3 Die fünf Einstufungskategorien

HU-RAC 1 – Baseline

Smarte Robotiksysteme ohne Personenbezug im Produktivbetrieb, geringe Gefährdung, keine KI-Hochrisiko-Einstufung, keine vulnerablen Zielgruppen. Typische Denkbeispiele: Mähroboter im Privatgarten, Pool-Reinigungsroboter, autonome Rasenbewässerung, einfache Agrar-Outdoor-Roboter auf abgegrenzten Flächen.

HU-RAC 2 – Enhanced

Systeme mit Umgebungssensorik, die technisch Personen erfassen kann, aber nicht primär für biometrische Identifikation eingesetzt wird. In privaten oder gewerblich-geschlossenen Räumen. Typische Denkbeispiele: Saugroboter, Fensterputzroboter, einfache Indoor-Drohnen, Haushalts-Assistenzroboter ohne Companion-Funktion, Lagerlogistik-Systeme in geschlossenen Bereichen.

HU-RAC 3 – Professional

Gewerblich-industrieller Einsatz mit ERP- oder Prozessintegration, oder gewerbliche Umgebungen mit Publikumskontakt ohne vulnerable Zielgruppen. Typische Denkbeispiele: Cobots und Industrieroboter mit Mensch-Roboter-Kollaboration, Schweißroboter in der Schwerindustrie, Logistik-Humanoide, prozessintegrierte KI-Brücken, Reinigungsroboter im öffentlichen Raum, Kochroboter in der Gastronomie, autonome Lieferroboter im Last-Mile-Bereich.

HU-RAC 4 – Sensitive

Einsatz in Pflege, Gesundheit, Bildung, Kinderbetreuung oder mit biometrischer Datenerfassung und/oder vulnerablen Zielgruppen. Typische Denkbeispiele: Companion- und Pflegeroboter in Seniorenresidenzen und häuslichen Pflegesituationen, OP-Assistenzsysteme, Therapieroboter, Roboter in Kinderbetreuungseinrichtungen, Wachroboter mit Personenerkennung, humanoide Hausassistenten in Betreuungskontexten.

HU-RAC 5 – Critical / Sovereign

Militärische oder Dual-Use-Anwendungen, Einsatz in kritischen Infrastrukturen, Hochrisiko-Einsätze mit staatlicher oder rechtlich besonders geschützter Sensitivität (Justiz, Strafverfolgung, nachrichtendienstliches Umfeld). Diese Kategorie ist im Modell bewusst vorgesehen, auch wenn ihre Ausgestaltung im Wesentlichen durch spezialisierte Regelwerke (BSI-Vorschriften, NATO-STANAGs, nationale VS-Regelungen) erfolgt. Das Denkmodell bildet hier nur den zivilen Rahmen ab, auf den diese Spezialregelwerke aufsetzen können.

5 Erwartungsmatrix zur Diskussion

Der folgende Abschnitt übersetzt die fünf Kategorien in ein differenziertes Erwartungsprofil – beschränkt auf die Felder Datenhoheit, Datensicherheit, regulatorische Einordnung, KI-Bezug und Betroffenenenschutz. Die Matrizen sind als Illustrationsangebot gedacht, wie ein abgestuftes Regime aussehen könnte – nicht als Liste verbindlicher Pflichten.

Erwartungen aus dem Bereich der technischen und funktionalen Sicherheit (Notaus-Logik, Power-and-Force-Limiting, dynamische Stabilität, Stromausfallverhalten) sind bewusst nicht abgebildet. Sie werden im angekündigten zweiten Impulspapier eigenständig behandelt. Wo in den folgenden Matrizen gelegentlich Normen zitiert werden, die in den Maschinensicherheitsbereich hineinreichen (etwa bei Kennzeichnung oder Transparenz), geschieht dies nur, soweit sie auch datenschutz- oder informationsrechtlich relevant sind.

Legende

E-Min	Minimal essenziell – in dieser Kategorie überwiegend bereits durch geltendes Recht (DSGVO, AI Act, MVO, CRA) oder etablierten Marktstandard erwartet.
E-Plus	Essenziell für konservative Grundrechts- und Resilienzsicherheit – geht über den gegenwärtigen Marktstandard hinaus, wird in dieser Kategorie als aspirationell-notwendig betrachtet.
R	Empfohlen – wird regelmäßig empfohlen, aber nicht einheitlich als unverzichtbar gesehen.
O	Optional – wird in der Fachdiskussion erwogen, ist aber ohne einheitliche Erwartungshaltung.
–	In der Diskussion nicht regelmäßig aufgeworfen für diese Kategorie.

Die Aufspaltung in E-Min und E-Plus ermöglicht eine realistische Selbsteinschätzung: Startups und KMU können mit E-Min beginnen und E-Plus als Entwicklungsroadmap deklarieren, ohne aus der HU-RAC-Kategorie zu fallen. Die Matrizen sind kumulativ gedacht: Eine höhere Kategorie umfasst die darunterliegenden Überlegungen und fügt weitere hinzu.

5.1 Datensouveränität und Datenschutz

Betrachtungspunkt	HU-RAC 1	HU-RAC 2	HU-RAC 3	HU-RAC 4	HU-RAC 5
Datenverarbeitung in EU/CH	R	E-Min	E-Min	E-Min	E-Min
Unabhängigkeit von US-Hyperscalern	–	R	E-Plus	E-Plus	E-Min
Vollständige AVV nach Art. 28 DSGVO	R	E-Min	E-Min	E-Min	E-Min
Art.-48-DSGVO-Klausel	–	E-Plus	E-Min	E-Min	E-Min
Offenlegung Unterauftragsverarbeiter	–	E-Min	E-Min	E-Min	E-Min
Zustimmungsvorbehalt bei Änderungen	–	–	E-Plus	E-Min	E-Min
Warrant-Canary / Transparenzpflicht	–	–	R	E-Plus	E-Plus
Art.-9-DSGVO-Konzept bei Biometrie	–	–	R	E-Min	E-Min
DSFA mit Datenflussdokumentation	–	–	R	E-Min	E-Min
Souveräne Cloud (C5-zertifiziert)	–	–	O	R	E-Min

5.2 KI-Bezug nach KI-Verordnung

Betrachtungspunkt	HU-RAC 1	HU-RAC 2	HU-RAC 3	HU-RAC 4	HU-RAC 5
Dokumentierte KI-Einstufung	–	E-Min	E-Min	E-Min	E-Min

Betrachtungspunkt	HU-RAC 1	HU-RAC 2	HU-RAC 3	HU-RAC 4	HU-RAC 5
Technische Dokumentation Art. 11	–	–	E-Min	E-Min	E-Min
Aufzeichnungspflichten Art. 12	–	–	E-Min	E-Min	E-Min
Transparenzpflicht Art. 13	–	–	E-Min	E-Min	E-Min
Menschliche Aufsicht Art. 14	–	–	E-Min	E-Min	E-Min
Erklärbarkeit sicherheitskrit. Entsch.	–	–	R	E-Plus	E-Plus
ISO/IEC 42001 (KI-Managementsystem)	–	–	O	R	E-Plus
KI-Readiness-Testat durch Dritte	–	–	O	E-Plus	E-Plus
Opt-out für kontinuierliches Feldlernen	–	E-Min	E-Min	E-Min	E-Min
Kein impliziter Lernaustausch zwischen Kunden	–	R	E-Min	E-Min	E-Min

5.3 Cybersicherheit

Betrachtungspunkt	HU-RAC 1	HU-RAC 2	HU-RAC 3	HU-RAC 4	HU-RAC 5
CRA-Readiness (VO 2024/2847)	E-Min	E-Min	E-Min	E-Min	E-Min
Software Bill of Materials (SBOM)	–	R	E-Min	E-Min	E-Min
Vulnerability-Disclosure-Prozess	–	R	E-Min	E-Min	E-Min
CVE-Monitoring und Response	–	R	E-Min	E-Min	E-Min
Signierte Updates mit Rollback	E-Min	E-Min	E-Min	E-Min	E-Min
Korruptionsschutz nach MVO	R	E-Min	E-Min	E-Min	E-Min
Incident-Reporting mit SLAs	–	R	E-Min	E-Min	E-Min
Bug-Bounty-Programm	–	–	R	E-Plus	E-Plus
ISO/IEC 27001	–	O	R	E-Min	E-Min
BSI-Grundschutz-Zertifizierung	–	–	O	E-Plus	E-Min

5.4 Schlüsselhoheit und Zero-Knowledge

Betrachtungspunkt	HU-RAC 1	HU-RAC 2	HU-RAC 3	HU-RAC 4	HU-RAC 5
Transportverschlüsselung (TLS 1.3)	E-Min	E-Min	E-Min	E-Min	E-Min
Datenverschlüsselung at rest	R	E-Min	E-Min	E-Min	E-Min
Bring Your Own Key (BYOK)	–	O	E-Plus	E-Min	E-Min
Hold Your Own Key (HYOK)	–	–	R	E-Plus	E-Min
Hardware Root of Trust (TPM/SE)	–	–	R	E-Plus	E-Min
Kundenseitiges HSM	–	–	O	E-Plus	E-Min
Zero-Knowledge-Architektur	–	–	O	E-Plus	E-Plus
M-of-N Recovery (Shamir Secret Sharing)	–	–	–	E-Plus	E-Plus
Unabhängiges Kryptografie-Audit	–	–	–	E-Plus	E-Plus
BSI TR-03145 (Secure CA)	–	–	O	R	E-Plus

5.5 Mandantentrennung und Backend-Sicherheit

Betrachtungspunkt	HU-RAC 1	HU-RAC 2	HU-RAC 3	HU-RAC 4	HU-RAC 5
Single-Tenant-Deployment	–	R	E-Plus	E-Min	E-Min

Betrachtungspunkt	HU-RAC 1	HU-RAC 2	HU-RAC 3	HU-RAC 4	HU-RAC 5
Zero-Trust-Autorisierung auf API-Ebene	–	E-Min	E-Min	E-Min	E-Min
Externe Pen-Tests Autorisierungslogik	–	–	R	E-Min	E-Min
Red-Team-Übungen Mandantentrennung	–	–	O	E-Plus	E-Min
Getrennte Netzsegmente (OT-VLAN)	–	R	E-Min	E-Min	E-Min
Session-Recording bei Remote-Support	–	–	R	E-Min	E-Min
Kundenseitig initiiertes Remote-Support	–	–	E-Min	E-Min	E-Min
Öffentlicher Disclosure-Prozess	–	–	R	E-Plus	E-Plus

5.6 Betroffenenenschutz, Transparenz und Ethik

Betrachtungspunkt	HU-RAC 1	HU-RAC 2	HU-RAC 3	HU-RAC 4	HU-RAC 5
Transparente Kennzeichnung als Roboter	R	E-Min	E-Min	E-Min	E-Min
Opt-out Datenübertragung	R	E-Min	E-Min	E-Min	E-Min
Abschaltbare Telemetrie	–	E-Min	E-Min	E-Min	E-Min
Verzicht auf biometr. Dauerüberwachung	–	E-Min	E-Min	E-Min	E-Min
Kinderschutzkonzept bei Zielgruppe	–	–	–	E-Min	E-Min
Ethik-Komitee-Einbindung (Pflege)	–	–	–	E-Min	E-Min
Würdeerhaltungsprinzipien dokumentiert	–	–	–	E-Plus	E-Plus

Zeilen zu Notaus, Normal-Stopp-Funktion und Gewaltschutz-Abschaltung sind hier bewusst nicht aufgeführt. Sie gehören in den Bereich der technischen und funktionalen Sicherheit und werden im angekündigten zweiten Impulspapier behandelt.

5.7 Normungsanschluss und Zukunftsfähigkeit

Betrachtungspunkt	HU-RAC 1	HU-RAC 2	HU-RAC 3	HU-RAC 4	HU-RAC 5
Umsetzung neuer Normen binnen 12 Monaten	–	R	E-Min	E-Min	E-Min
Proaktive Benachrichtigung bei Updates	–	R	E-Min	E-Min	E-Min
Offene Schnittstellen (ROS2 o.ä.)	–	O	R	E-Plus	E-Plus
Mitarbeit ISO TC 299 WG 12	–	–	O	R	R
Mitarbeit DIN NA 060-30	–	–	O	R	R
Mitarbeit CEN/CENELEC JTC 21	–	–	O	R	R
Mitarbeit ETSI TC CYBER	–	–	O	R	R
Jährlicher Transparenzbericht	–	–	R	E-Plus	E-Plus

6 Zwei weitere Betrachtungsebenen

6.1 Business-Kritikalität

Die HU-RAC-Kategorie allein bildet die Verletzungs- und Regulierungsrisiken ab. Sie bildet noch nicht ab, wie kritisch der Ausfall des Systems für den Betreiber ist. Ein HU-RAC-3-Cobot in getakteter Fertigung und ein HU-RAC-3-Forschungsroboter sind regulatorisch gleichgestellt, aber betrieblich extrem unterschiedlich. Ein Ausfall im ersten Fall bedeutet Produktionsstillstand, im zweiten nur eine verschobene Versuchsreihe.

Das Denkmodell sieht deshalb eine orthogonale Business-Kritikalität-Einstufung mit drei Ebenen vor:

Level A	Prozess- oder sicherheitskritisch. Ausfall führt zu Produktionsstillstand, Patientengefährdung oder Lieferketten-Unterbrechung. Denkbeispiele: ERP-integrierte Automatisierungs-Brücke, OP-Assistenz, industrieller Cobot in getakteter Fertigung, Pflege-Companion in unbetreuter Wohnsituation, KRITIS-Inspektionsroboter.
Level B	Betriebswichtig, aber überbrückbar. Denkbeispiele: Lagerlogistik mit manueller Fallback-Option, Reinigungsroboter im Gewerbe, Gastro-Kochroboter, Agrarroboter.
Level C	Nicht kritisch. Ausfall tolerierbar. Denkbeispiele: Forschungsroboter, Demogeräte, Einzelplatz-Automatisierung, private Haushaltsroboter.

Operationalisierung der Level

Um die Einstufung weniger subjektiv und damit vergleichbarer zu machen, werden folgende Orientierungskriterien vorgeschlagen. Ein Level A liegt vor, sofern mindestens eine der folgenden Bedingungen erfüllt ist:

- Das System trägt zu mehr als 20 % zur betrieblichen Kernleistung oder zum Umsatz des Betreibers bei.
- Ein Ausfall von mehr als vier Stunden führt zu einer Patientengefährdung, einer Unterbrechung einer medizinisch notwendigen Versorgung oder einem KRITIS-Ausfall.
- Der Betrieb unterliegt gesetzlichen Verfügbarkeitspflichten (z.B. aus KRITIS-Dachgesetz, SGB, Medizinproduktrecht) mit definierten Service-Levels.
- Die Wiederherstellung nach einem Ausfall erfordert mehr als 72 Stunden oder externe Dienstleister.

Level B liegt vor, wenn das System betriebswichtig ist, ein Ausfall aber durch manuelle oder alternative Verfahren innerhalb von 24 Stunden überbrückbar bleibt und keine Patientengefährdung entsteht. Level C liegt vor, wenn ein Ausfall den Betrieb nicht unmittelbar beeinträchtigt und keine Dritten betroffen sind.

Mindest-Standards für den Degradet-Mode

Die Kombination aus HU-RAC-Kategorie und Business-Kritikalität-Level gibt einen nachvollziehbaren Rahmen für Mindeststandards im Weiterbetrieb bei Ausfall der Hersteller-Cloud vor:

HU-RAC × Level	Mindest-Cloud-Autonomie	Weitere Anforderungen
HU-RAC 4 × A	24 Monate	Grundfunktionen lokal; Datenexport jederzeit möglich; Source- und Daten-Escrow verpflichtend
HU-RAC 4 × B	12 Monate	Grundfunktionen lokal; Datenexport; Source-Escrow

		empfohlen
HU-RAC 3 × A	12 Monate	Kernbetrieb lokal; Datenexport; Exit-Klauseln vertraglich
HU-RAC 3 × B	6 Monate	Kernbetrieb lokal; Datenexport
HU-RAC 2 × C	Empfohlen	Datenexport einfach möglich; Degraded Mode optional

Die Schwellenwerte sind als diskutierbare Orientierung gedacht und in konkreten Normungsverfahren verfeinerungsfähig.

6.2 Betriebskontinuität und Anbieter-Resilienz

Insolvenzen cloudabhängiger Anbieter in angrenzenden Marktsegmenten (siehe Kapitel 1.1) legen nahe, dass die Resilienz des Anbieters und die Kontinuität des Betriebs eigenständige Betrachtungsdimensionen verdienen. Das Denkmodell schlägt drei ineinandergreifende Mechanismen vor, deren Intensität mit der HU-RAC-Kategorie und dem Business-Kritikalitäts-Level skaliert.

Architektonische Kontinuität

- Ab HU-RAC 2 erscheint die Fähigkeit zum Weiterbetrieb ohne Cloud (Degraded Mode) sinnvoll.
- Ab HU-RAC 3 scheinen offene Schnittstellen (ROS2 oder gleichwertig) und Datenportabilität in Standardformaten angemessen.
- Ab HU-RAC 4 erscheint eine On-Premises-Betriebsoption diskussionswürdig, die mindestens 24 Monate ohne Hersteller-Cloud funktioniert.
- Bei HU-RAC 5 wäre Air-Gap-Fähigkeit zu erwarten.

Vertragliche Kontinuität

Einfacher Datenexport-Anspruch bereits ab HU-RAC 1, Source-Code-Escrow ab HU-RAC 3 (insbesondere bei Level A), Daten-Escrow und Cloud-Kontinuitätsgarantie ab HU-RAC 4. Die konkrete Vertragsgestaltung liegt außerhalb des Impulsgedankens und wäre anwaltlich auszugestalten.

Anbieter-Resilienz-Rating

Drei Klassen, die aus finanzieller Stabilität, Eigentümerstruktur und operativer Resilienz abgeleitet werden: R1 (etablierter Konzern), R2 (stabiler Mittelständler), R3 (Start-up mit erhöhtem Insolvenz- oder Change-of-Control-Risiko). Bei HU-RAC 4 und 5 wäre R3 nur bei voll ausgestalteten Kontinuitätsmechanismen vertretbar.

7 Rolle der Betreiber

Das Denkmodell spricht bislang primär zu Herstellern und Normungsakteuren. In der praktischen Anwendung sind es jedoch oft die Betreiber – Krankenhäuser, Pflegeheime, Industriebetriebe, kommunale Einrichtungen – die über Erfolg oder Scheitern einer Robotik-Einführung entscheiden. Sie wählen aus, beschaffen, betreiben, dokumentieren und haften mit. Eine Klassifikationssystematik, die diese Perspektive ausspart, bleibt unvollständig.

7.1 Verantwortlichkeitsverteilung entlang der HU-RAC-Logik

Die Rollenverteilung zwischen Hersteller und Betreiber folgt in der Regel bereits bestehendem Recht. Das Denkmodell lässt sich ohne rechtliche Änderungen in diese Verteilung einfügen:

- Hersteller sind typischerweise Verantwortliche im Sinne von Art. 4 DSGVO für die Produktentwicklung, für die technische Dokumentation nach AI Act und MVO sowie für die Konformitätserklärung. In der HU-RAC-Logik liefern sie die Klassifikationsgrundlage: Sie stufen ihr Produkt vor, belegen die Einstufung nachvollziehbar und benennen, welche Erwartungen in welcher Kategorie erfüllt sind.
- Integratoren (Systemhäuser, Implementierungspartner) tragen die Verantwortung für die Einbettung in die jeweilige IT-Landschaft, für Schnittstellen zu bestehenden Systemen und für die technische Konfiguration. In der HU-RAC-Logik stellen sie sicher, dass die Einstufung auch nach der Integration gültig bleibt – etwa dass eine Mandantentrennung nicht durch Konfigurationsfehler unterlaufen wird.
- Betreiber sind Verantwortliche im Sinne von Art. 4 DSGVO für den Einsatzkontext. Sie schließen Auftragsverarbeitungsverträge nach Art. 28 DSGVO, führen DSFA nach Art. 35 DSGVO, dokumentieren technische und organisatorische Maßnahmen und tragen die Betreiberpflichten nach MVO. In der HU-RAC-Logik prüfen sie, ob die Herstellereinstufung dem konkreten Einsatzkontext entspricht, und heben sie bei abweichendem Kontext gegebenenfalls an.

7.2 HU-RAC in Beschaffung und Vergabe

Für die praktische Verankerung in Beschaffungsprozessen könnte das Denkmodell an mehreren Stellen ansetzen:

- Leistungsbeschreibungen in Ausschreibungen könnten eine HU-RAC-Zielkategorie benennen und auf die zugehörige Erwartungsmatrix verweisen. Anbieter wären gehalten, ihre Selbsteinstufung plus Belege beizulegen.
- In Vergabeverfahren nach VgV könnten HU-RAC-Matrix-Kriterien als Eignungs- oder Zuschlagskriterien abgebildet werden, insbesondere im Gesundheits- und Sozialsektor sowie bei kommunalen KRITIS-nahen Beschaffungen.
- Bei Verträgen mit längerer Laufzeit (Leasing, Miete, Servicemodelle) könnten Exit-Klauseln, Datenportabilitäts-Garantien und Eskalationsmechanismen an der HU-RAC-Kategorie orientiert ausgestaltet werden.
- Betreiber-Richtlinien und Datenschutz-Managementsysteme könnten HU-RAC-Einstufungen als Eingangsgröße für die interne Risikobewertung und für die Ausgestaltung der technischen und organisatorischen Maßnahmen nutzen.

7.3 Ein kurzer Hinweis zur Praxistauglichkeit

Für kleinere Betreiber – kommunale Träger, Pflegeeinrichtungen mittlerer Größe, Kliniken ohne zentrale IT-Abteilung – ist die Vielzahl der Anforderungen in Kapitel 5 potenziell überfordernd. Die E-Min-/E-Plus-Aufspaltung adressiert dieses Problem teilweise: Ein

Betreiber kann sich an die E-Min-Spalten als Mindest-Auswahlkriterien halten und E-Plus als Differenzierungsmerkmal werten. Die Verbände der jeweiligen Branchen (Pflegeverbände, Krankenhausgesellschaften, kommunale Spitzenverbände) könnten beim Uptake unterstützen, indem sie sektorspezifische Beschaffungsleitfäden auf HU-RAC-Basis erarbeiten.

8 Wirkung des Denkmodells: Marktöffnung statt Pflichtenheft

Eine Klassifikationssystematik wirkt nicht nur als Bürde, sondern auch als Brücke. Wer als Anbieter heute einen Pflegeroboter entwickelt, muss gegen eine diffuse Wolke aus Regulierungsunsicherheit anarbeiten. Welche Datenschutzmaßnahmen sind in Pflegesituationen angemessen? Welche Kryptografie-Architektur wird erwartet? Welches Niveau an Erklärbarkeit bei KI-gestützten Entscheidungen ist angezeigt? Die Antworten auf diese Fragen sind heute Gesprächsabsagen mit Einkäufern, gekippte Pilotprojekte, gescheiterte Investorenrunden. Jede dieser Antworten kostet den Markt Zeit und Kapital.

Ein klares Einstufungsmodell senkt diese Reibung. Der Anbieter weiß, in welcher Kategorie sich sein Produkt bewegt. Der Beschaffer weiß, welches Erwartungsprofil angemessen ist. Der Investor kann die regulatorischen Kapital- und Zeitkosten einschätzen. Die Marktaufsicht hat einen Bezugsrahmen, der Plausibilität prüfbar macht.

Die Gegenüberstellung mit dem RARI-Framework unterstreicht dieses Argument. Branchen mit breitem regulatorischen Korridor – Healthcare, Home – sind zugleich die mit der niedrigsten kommerziellen Adoptionsreife. Das ist kein Zufall. Die regulatorische Unsicherheit ist ein Teil der Adoptionsreibung. Ein Denkmodell, das den Korridor nachvollziehbar schließt, wirkt damit zugleich als Marktöffnungs-Instrument.

Anders gesagt: Eine solche Systematik ist volkswirtschaftlich ein Investment in Markterschließung, nicht nur ein Compliance-Kostenpunkt. Diese Doppelwirkung wäre aus Sicht der Autorin ein lohnendes Leitmotiv für die weitere Diskussion und gegebenenfalls für eine spätere Überführung in ein Normungsverfahren.

9 Wo das Denkmodell anschlussfähig wäre

Dieses Impulspapier ist keine Norm und soll keine werden wollen – es sei denn, die Resonanz aus Fachkreisen macht den Schritt plausibel. Für diesen Fall sind folgende Anschlussmöglichkeiten denkbar:

- Ein Impulsgespräch mit DIN NA 060 (Robotik) über die Eignung des Denkmodells als Ausgangspunkt für eine DIN SPEC nach dem PAS-Verfahren.
- Eine inhaltliche Diskussion mit ISO TC 299 WG 12, die sich mit humanoiden und dynamisch stabilen Systemen befasst.
- Ein wissenschaftlicher Beitrag in Kooperation mit Fraunhofer IAO oder IPA, der die ökonomische Wirkungsthese (Marktöffnung durch Klassifikation) empirisch belegt oder widerlegt.
- Eine Gesprächsspur mit BSI hinsichtlich der Kryptografie- und Zero-Knowledge-Aspekte in HU-RAC 4 und 5.
- Eine Resonanzschleife mit Persona AI und anderen Industriepartnern, die bereits an Adoptions-Reifegrad-Modellen arbeiten.
- Eine Einbindung zivilgesellschaftlicher Stimmen (Datenschutzaufsicht, Stiftung Datenschutz, Bitkom, Pflegeverbände, Patientenvertretungen).
- Die Veröffentlichung des angekündigten zweiten Impulspapiers zur technischen und funktionalen Sicherheit, das die in Kapitel 2 ausgewiesenen Lücken adressieren wird.

Die Autorin sieht dieses Papier nicht als ihr letztes Wort, sondern als Einladung zur Diskussion. Rückmeldungen, Kritik und Erweiterungsvorschläge sind ausdrücklich willkommen. Beiträge zu den in Kapitel 2 skizzierten offenen Fragen der technischen Sicherheit sind besonders willkommen und fließen in die Vorbereitung des zweiten Papiers ein.

Annex A – Die fünf kommerziellen Dimensionen (RARI-Bezug)

Dieser Annex ergänzt das regulatorisch-risikoorientierte Denkmodell um die kommerziell-operative Perspektive. Als Referenz dient das RARI-Framework (Robot Adoption Readiness Index), vorgestellt durch Nicolaus Radford, CEO von Persona AI, auf dem Humanoids Summit 2025, Mountain View (Kalifornien), am 11. Dezember 2025.

A.1 Die fünf Bewertungsdimensionen

Labor Scarcity	Fachkräftemangel im Einsatzsegment. Hohe Knappheit erhöht die Zahlungsbereitschaft und den Druck zur Automatisierung.
Labor Cost	Lohnniveau im Einsatzsegment. Hohe Löhne rechtfertigen höhere Kapitalkosten für humanoide Ersatzarbeit.
Task Ease	Einfachheit und Klarheit der zu automatisierenden Aufgaben. Strukturierte, wiederholbare Aufgaben sind technisch zugänglicher.
Env. Predictability	Strukturiertheit und Vorhersagbarkeit der Arbeitsumgebung. Industrie- und Logistik-Umgebungen sind typischerweise strukturiert, häusliche Umgebungen nicht.
Dev. Ease	Entwicklungsaufwand für die branchenspezifische Anpassung. Geringe Entwicklungsreibung beschleunigt den Markteintritt.

A.2 Die acht RARI-Referenzbranchen mit normierten Scores

Branche	RARI-Score (0–100)	Adoptionsreife
Heavy Industry	100,0	sehr hoch
Automotive	96,9	sehr hoch
Warehousing	72,5	hoch
Construction	58,5	mittel
Healthcare	~ 40	niedrig-mittel
Retail/QSR	39,7	niedrig-mittel
Agriculture	39,7	niedrig-mittel
Home	nahe 0	sehr niedrig

Die Scores werden hier als Sekundärquelle zitiert, um die kommerzielle Perspektive transparent zu machen. Sie sind nicht Teil einer normativen Festlegung dieses Impulspapiers. Urheberschaft und Deutungshoheit liegen bei Persona AI.

Annex B – Zwölf Anwendungsdomänen im Überblick

Die Spannweite smarter Robotik lässt sich nicht auf einige wenige Anwendungsfelder reduzieren. Der folgende Überblick erweitert die acht RARI-Branchen um vier weitere Felder (Logistics/Last-Mile, Hospitality, Public Sector/Security, Defence/Dual-Use), um die Vielfalt angemessen abzubilden. Zu jeder Domäne wird eine typische HU-RAC-Bandbreite, eine qualitative Adoptionsreife-Einschätzung und ein Verweis auf relevante rechtliche Zusatzebenen angegeben.

Domäne	HU-RAC-Spanne	Adoptionsreife	Rechtliche Zusatzebenen
Heavy Industry	3	sehr hoch	ATEX-RL 2014/34/EU; BetrSichV; BG RCI-Regeln
Automotive	3	sehr hoch	ISO 26262; TISAX; UN-R155/156 bei Fahrzeugintegration
Warehousing	2–3	hoch	GDP; ISO 13485 bei Pharma/Medizinlogistik; IFS/BRC bei Lebensmittel
Construction	3	mittel	BauPVO (EU) 305/2011; BG-BAU-Regeln; ArbStättV; Baustellenverordnung
Healthcare	2–5	niedrig-mittel	MDR (EU) 2017/745; MPDG; MPBetreibV; IEC 60601-Familie; SGB V/XI
Retail/QSR	2–3	niedrig-mittel	LMHV bei Lebensmittelkontakt; LFGB; PAngV; JuSchG bei Kinderkontakt
Agriculture	1–3	niedrig-mittel	VO (EU) 167/2013; DüV; PflSchG; Agrarstatistikgesetz
Home	1–4	sehr niedrig	Haushaltsausnahme Art. 2(2)(c) DSGVO; ProdSG
Logistics / Last-Mile	2–3	hoch	StVO (öffentl. Raum); LuftVG/EU 2018/1139 bei Drohnen; Transportrecht
Hospitality	2–3	mittel	Gaststättengesetz; LMHV; BGG (Barrierefreiheit); DSGVO bei Gastdaten
Public Sector / Security / Emergency	4–5	mittel	PolG der Länder; BKAG; SUG; BSIG; KRITIS-Dachgesetz
Defence / Dual-Use	5	nicht zutreffend	Dual-Use-VO 2021/821; AWG/AWV; BSI-VS-Vorschriften; NATO STANAGs

Annex C – Acht Illustrationsbeispiele

Die folgenden Beispiele illustrieren, wie das Denkmodell in konkreten Fällen anwendbar wäre. Sie sind bewusst als Illustration gedacht und ersetzen nicht die Einzelfall-Analyse. Die Beispiele C.6 bis C.8 behandeln gezielt Grenzfälle, an denen die Tragfähigkeit des Modells unter komplexen Bedingungen sichtbar wird.

C.1 Mähroboter im Privatgarten

Einsatzumgebung privat-outdoor (niedrig), Bauart radbasiert (niedrig), Datenkategorien Telemetrie (niedrig), KI-Risiko bagatelhaft (niedrig), physisches Gefährdungspotenzial PFL-Klasse (niedrig), Betroffenenkreis nur Betreiber (niedrig). Höchster Wert niedrig. Illustrative Einstufung: HU-RAC 1, Level C. Domäne: Home.

C.2 Industrieller Cobot mit ERP-Integration

Einsatzumgebung industriell-Fertigung (mittel), Bauart stationär (mittel), Datenkategorien Prozessdaten mit Personenbezug (mittel), KI-Risiko Hochrisiko nach AI Act (hoch), physisches Gefährdungspotenzial Cobot-Klasse (mittel), Betroffenenkreis Mitarbeitende (mittel). Höchster Wert hoch auf der KI-Achse. Illustrative Einstufung: HU-RAC 3, Level A. Domäne: Heavy Industry oder Automotive.

C.3 Pflege-Companion in Seniorenresidenz

Einsatzumgebung sensibel-Pflege (sehr hoch), Bauart mobil oder dynamisch stabil (hoch), Datenkategorien biometrisch und intime Langzeitbeobachtung (sehr hoch), KI-Risiko Hochrisiko mit vulnerabler Zielgruppe (sehr hoch), physisches Gefährdungspotenzial mittel bis hoch, Betroffenenkreis vulnerable Personen (sehr hoch). Höchster Wert sehr hoch auf mehreren Achsen. Illustrative Einstufung: HU-RAC 4, typisch Level A, R1 oder R2 angezeigt. Domäne: Healthcare mit MDR-Prüfung je nach Zweckbestimmung.

C.4 Autonomer Lieferroboter im Last-Mile-Betrieb

Einsatzumgebung gewerblich mit Publikumskontakt (hoch), Bauart radbasiert mobil (mittel), Datenkategorien Umgebungssensorik mit Personenerfassung (mittel), KI-Risiko begrenzt bis Hochrisiko (mittel-hoch), physisches Gefährdungspotenzial mittel, Betroffenenkreis unbeteiligte Dritte (hoch). Höchster Wert hoch. Illustrative Einstufung: HU-RAC 3, Level B. Domäne: Logistics/Last-Mile.

C.5 Inspektionsroboter in kritischer Infrastruktur

Beispiel Umspannwerk, Netzleitwarte oder Wasserwerk: Einsatzumgebung KRITIS-sensibel (sehr hoch), Bauart variabel (mittel), Datenkategorien staatssicherheitsrelevante Betriebsdaten (sehr hoch), KI-Risiko Hochrisiko mit staatlicher Sensitivität (sehr hoch), physisches Gefährdungspotenzial mittel, Betroffenenkreis betreiberseitig (mittel). Illustrative Einstufung: HU-RAC 5, Level A, R1 empfohlen. Domäne: Public Sector / Security / Emergency mit BSI-KritisV-Bezug.

C.6 Forschungsroboter an einer Universitätsklinik (Grenzfall)

Ein humanoides Forschungssystem wird in einer Universitätsklinik zur Erprobung eines neuen Pflege-Interaktionskonzepts eingesetzt. Ohne Kontextbetrachtung wäre die Einstufung HU-RAC 4 (vulnerable Zielgruppe, sensitive Einsatzumgebung). Der Einsatz erfolgt jedoch unter Ethikkommissions-Begleitung, mit begrenztem Personenkreis, expliziten Einwilligungen nach Art. 9 Abs. 2 lit. a DSGVO und unter den Forschungsausnahmen nach

Art. 89 DSGVO. Gemäß der zweiten Ausnahmeregel in Kapitel 4.2 kann die Einstufung für die Dauer der Forschung um eine Stufe reduziert werden. Illustrative Einstufung: HU-RAC 3 für die Forschungsphase, mit dokumentierter DSFA, Level B, R2 oder R1. Beim Übergang in den Regelbetrieb greift wieder HU-RAC 4. Lehre: Das Modell bleibt auch in Forschungskontexten anwendbar, ohne die Forschungsfreiheit unverhältnismäßig einzuschränken.

C.7 Consumer-Humanoid mit optionalem Abo-Service (Grenzfall)

Ein humanoider Assistenzroboter für den Privathaushalt wird als Consumer-Produkt vermarktet (Basisfunktion offline, Home-Domäne, Haushaltsausnahme nach Art. 2 Abs. 2 lit. c DSGVO). Optional ist ein Cloud-Abo mit erweiterten Funktionen (Routinenlernen, Spracherkennung, Fernzugriff für Angehörige) zubuchbar. Ohne Abo liegt die Einstufung bei HU-RAC 2 (Bauart humanoid, Sensorik mit Personenerfassung, aber Haushaltsausnahme greift). Mit Abo entfällt die Haushaltsausnahme, weil der Anbieter als Verantwortlicher die Daten verarbeitet – die Einstufung hebt sich auf HU-RAC 3 bis 4, abhängig vom Umfang der biometrischen Verarbeitung und der Zielgruppe (Kinder, ältere Menschen im Haushalt). Zusätzlich greift bei Insolvenz des Anbieters das Plattform-Risiko: ohne Abo bleibt das Gerät funktionsfähig, mit Abo verliert es seine Kernfunktionen. Illustrative Einstufung: HU-RAC 2 im Grundzustand, HU-RAC 3-4 bei aktivem Abo; Level B bis A je nach Haushaltskontext. Lehre: Dynamische Einstufungen sind denkbar, müssen aber vertraglich und technisch sauber ausgewiesen sein.

C.8 Krankenhauslogistikroboter in Mischumgebung (Grenzfall)

Ein autonomer Lieferroboter verteilt Medikamente, Proben und Wäsche zwischen Stationen. Er bewegt sich sowohl in nicht-öffentlichen Versorgungskorridoren als auch in halböffentlichen Bereichen (Aufzüge, Flure mit Patientenverkehr). Die Datenkategorien umfassen Transportprotokolle mit Patientenbezug (Probenzuordnung), aber keine direkte Biometrie. Einsatzumgebung Mischung aus sensibel und Publikum (hoch), Bauart radbasiert (mittel), Datenkategorien mittelbar patientenbezogen (mittel-hoch), KI-Risiko begrenzt bis Hochrisiko (mittel), physisches Gefährdungspotenzial mittel, Betroffenenkreis gemischt (mittel-hoch). Nach der Regel der stärksten Belastung: HU-RAC 3 für den Regelbetrieb. Nach der zweiten Aggregationsregel (mehrere mittlere Achsen kumuliert) wird mindestens HU-RAC 3 erreicht – hier besonders plausibel wegen der Mischumgebung. Illustrative Einstufung: HU-RAC 3, Level A wegen Medikamentenlogistik-Kritikalität. Lehre: Mischumgebungen sind nicht durch eine einzelne Höchsteinstufung hinreichend charakterisiert; die Ergänzungsregel der Kapitel 4.2 greift und hebt die Einstufung, wo die Einzelachsen das nicht allein leisten.

Annex D – Quellen und Lektüreempfehlungen

D.1 Rechtsakte

- Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung
- Verordnung (EU) 2023/1230 – Maschinenverordnung
- Verordnung (EU) 2024/1689 – KI-Verordnung
- Verordnung (EU) 2024/2847 – Cyber Resilience Act
- Richtlinie (EU) 2024/2853 – Produkthaftungsrichtlinie
- Verordnung (EU) 2021/821 – Dual-Use-Verordnung

D.2 Technische Normen und Regelwerke

- ISO 10218-1/-2:2025 – Sicherheitsanforderungen für Roboter
- ISO/DIS 25785-1 – Sicherheit dynamisch stabiler mobiler Roboter
- ISO 13482 – Sicherheitsanforderungen für persönliche Pflegeroboter
- EN ISO 12100 – Risikobeurteilung
- ISO 13849-1 – Performance Levels
- ISO/IEC 42001 – KI-Managementsystem
- BSI TR-03145 und BSI C5

D.3 Fachliteratur und Industrieberichte

- Radford, N. (2025): Humanoid Adoption Readiness – Das RARI-Framework. Keynote, Humanoids Summit 2025, Mountain View, 11.12.2025. Persona AI Inc.
- Morgan Stanley Research (2025): Humanoid Robotics – The Future of Labor (A. Jonas et al.).
- IDTechEx (2025): Humanoid Robots 2025–2035: Technologies, Markets and Opportunities.
- Bain & Company (2025): Humanoid Robots – From Demos to Deployment. Technology Report 2025.
- Yole Group (2025): Humanoid Robots 2025 – The Race to Useful Intelligence.

D.4 Verwandte Klassifikationsansätze

Die folgenden Ansätze adressieren angrenzende Klassifikations- und Governance-Fragen in der Robotik. Keiner von ihnen kombiniert jedoch die für HU-RAC konstitutive Zusammenstellung aus Robotik-Einsatzkontext, Datenhoheits-Fokus und Overlay-Logik auf europäisches Recht. Das Feld ist damit für eine europäische Datenhoheits-Klassifikationssystematik offen.

Ontologische Governance-Klassifikation

- Ning, H.; Ding, J. (2026): Beyond Tools and Persons: Who Are They? Classifying Robots and AI Agents for Proportional Governance. arXiv:2604.05568. Das Modell verwendet die Cyber-Physical-Social-Thinking (CPST) space theory mit vier Dimensionen (computational, embodied, relational, cognitive) und einer Drei-Stufen-Taxonomie (Confined Actors, Socially-Aware Interactors, CPST-Integrated Agents). Governance-Fokus: Produkthaftung bis hin zu qualifizierter Rechtspersönlichkeit. Strukturell verwandt zu HU-RAC durch Mehrdimensionen-Aggregation; inhaltlich komplementär durch ontologischen statt kontextuellen Fokus.

Autonomie- und Intelligenz-Grading (Robotik und Fahrzeuge)

- SAE International (2018, fortgeschrieben): J3016 – Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems. Sechs Stufen (Level 0–5) der Fahrautomation. Methodisches Vorbild für HU-RAC's Stufen-Logik; inhaltlich nicht auf Datenhoheit bezogen.
- Haidegger, T. et al. (2024): Levels of Autonomy in Surgical Robotics (LASR). Systematic Review, FDA-gelistete chirurgische Roboter. Fünf Stufen von Robot Assistance bis Full Autonomy.
- SemiAnalysis (2025): Robotics Levels of Autonomy – Ein fünfstufiges Klassifikationsmodell für allgemeine Robotik, ausgerichtet auf kommerzielle Reife und Fähigkeiten entlang der Achsen Agency und Dexterity.
- Beijing Humanoid Robot Innovation Center (Mai 2025): T/CIE 298-2025 – Humanoid Robot Intelligence Grading Standard. Four-Dimension, Five-Level-Framework mit 22 Primärindikatoren. Adressiert Intelligenz-Grading, nicht Datenhoheit.
- Ministry of Industry and Information Technology (MIIT), China (Februar 2026): Humanoid Robot and Embodied Intelligence Standard System (2026 Edition). Nationaler Standardrahmen mit sechs Pfeilern. Weltweit erster staatlich getragener humanoider Robotik-Standardrahmen; Fokus auf technische Fähigkeit, Autonomie und Systemdesign.
- NLJIC/Shanghai (2024): Industriestandards mit vier technischen Leveln (L1–L4) und fünf Intelligenzleveln (G1–G5) für chinesische Humanoide.

Robotik-Privacy-Frameworks

- Google / Relford, E. (2024): Robotics Privacy Framework. Prinzipienorientierter Ansatz mit drei Schwerpunkten: Novel Interactions, Autonomous Engagement, Transparency. Keine abgestufte Klassifikation; Orientierungsrahmen statt Einstufungssystem.
- Rueben, M. et al. (2016): Privacy in Human-Robot Interaction – Survey. Klassifiziert Territorial-Bereiche in vier Kategorien (individual, shared, public, jurisdiction). Räumlich-territorialer Fokus, nicht datenhoheitlich.
- Fosch-Villaronga, E. (2021): Toward Privacy-Sensitive Human-Robot Interaction. Analyse der Privacy Policies acht führender Consumer-Robotik-Hersteller; kein Klassifikationsmodell, aber Evidenz für die Heterogenität heutiger Hersteller-Praxis.

Ethik- und Assurance-Standards

- IEEE 7000er-Familie (seit 2021): u.a. IEEE 7005 (Transparent Employer Data Governance), IEEE 7007 (Ontologically Driven Robotics), IEEE P7018 (Security/Trustworthiness Generative AI). Thematisch-ethische Standards ohne abgestufte Klassifikationslogik.
- BS 8611 (2016): Guide to the Ethical Design and Application of Robots and Robotic Systems. Prinzipientreibender britischer Standard zu Ethik-Aspekten (Privacy, Bias, Explainability, Worker Impact).

Data-Classification-Frameworks (angrenzend, nicht robotikspezifisch)

- Microsoft Service Assurance (laufend): Data Classification Framework. Drei- bis fünfstufige Datenklassifikation (Public, Internal, Confidential, Highly Confidential) mit zugeordneten Controls. Methodisches Vorbild für die Stufenlogik und E/R/O-Logik von HU-RAC; inhaltlich auf Unternehmensdaten, nicht auf Robotiksysteme bezogen.
- ISO 27701 (2019): Privacy Information Management System. Internationale Norm für Datenschutz-Managementsysteme, bildet die Basis für viele Privacy-Governance-Frameworks.

D.5 Relevante Vorfälle und Fälle

- Backend-Autorisierungsfehler bei einem marktführenden Hersteller autonomer Haushaltsroboter (Februar 2026): Fremdzugriff auf ca. 6.700 Geräte durch Fehler in der Mandantentrennung des MQTT-Backends.
- Rücknahme einer Zero-Knowledge-Cloud-Schutzfunktion durch einen marktbestimmenden US-Technologiekonzern in Großbritannien (Februar 2025) nach Anordnung britischer Sicherheitsbehörden.
- Insolvenz eines europäischen Herstellers vernetzter Blutdruckmessgeräte (2024): Verlust der Cloud-Infrastruktur und der Nutzerdaten als Muster cloudabhängiger Ausfälle; vergleichbare Fälle bei mehreren Smart-Home- und Connected-Health-Anbietern.

Annex E – Mapping-Schema: Orchestrierung bestehender Regelwerke

Das HU-RAC-Denkmodell versteht sich als Overlay auf bestehendes Recht (vergleiche Leitidee 4 in Kapitel 3.4). Der folgende Prozess in vier Schritten zeigt, wie HU-RAC in eine Einstufungsentscheidung eingebettet werden kann, ohne mit DSGVO, KI-Verordnung oder Maschinenverordnung in Konkurrenz zu treten. Das Schema ist als Arbeitsablauf für Hersteller, Integratoren und Betreiber gedacht.

E.1 Vier-Schritte-Prozess

Schritt	Regelwerk	Was zu prüfen ist
1	AI Act (VO 2024/1689)	Fällt das System in eine Hochrisiko-Kategorie nach Anhang III oder als Sicherheitskomponente? Greifen die Pflichten aus Art. 9 ff. (Risikomanagement, Datenqualität, Dokumentation, Logging, Transparenz, menschliche Aufsicht, Genauigkeit)?
2	HU-RAC-Einstufung	Einstufung in HU-RAC 1–5 entlang der sechs Achsen (Kapitel 4.1) unter Anwendung der Aggregationslogik (Kapitel 4.2). Bestimmung der Business-Kritikalität A/B/C (Kapitel 6.1) und der Anbieter-Resilienz-Klasse R1/R2/R3 (Kapitel 6.2).
3	DSGVO-Abgleich	Werden personenbezogene Daten verarbeitet? Wenn ja: Art. 6 Rechtsgrundlage, Art. 9 besondere Kategorien, Art. 28 AVV, Art. 35 DSFA-Pflicht (regelmäßig erforderlich ab HU-RAC 3), Art. 44 ff. Drittlandtransfer, Art. 48 Anordnungen von Drittstaaten.
4	HU-RAC-spezifische Controls	Ableitung zusätzlicher Erwartungen aus Kapitel 5: Schlüsselhoheit, Mandantentrennung, Betroffenenenschutz, Cybersicherheit, Normungsanschluss. Trennung in E-Min (Pflicht oder Marktstandard) und E-Plus (aspirationell, konservativ). Ergänzend: Sektorrecht (MDR, MPBetreibV, KRITIS-Dachgesetz, PoIG, SGB) und Maschinenverordnung (MVO 2023/1230).

E.2 Umgang mit Diskrepanzen

Es sind drei Konstellationen zu unterscheiden:

- AI-Act-Hochrisiko ohne entsprechende HU-RAC-Hochkategorie: kommt praktisch selten vor, ist aber denkbar. Anwendbar bleibt der AI Act mit seinen spezifischen Pflichten; HU-RAC tritt daneben und ergänzt um datenhoheitsbezogene Erwartungen.
- HU-RAC 4 oder 5 ohne AI-Act-Hochrisiko: typischer Fall bei Systemen mit nicht-KI-basierten Kernfunktionen in sensiblen Einsatzumgebungen. HU-RAC führt hier zu zusätzlichen, über den AI Act hinausgehenden Erwartungen an Schlüsselhoheit, Mandantentrennung und Betroffenenenschutz.
- Beide hoch: der Regelfall für humanoide Pflege- oder Medizinanwendungen mit adaptiven KI-Komponenten. Die Pflichten beider Rahmenwerke kumulieren; HU-RAC orientiert die Umsetzung kontextspezifisch.

E.3 Beispielhafte Anwendung: OP-Assistenzsystem

Schritt 1 AI Act: Hochrisiko (Anhang III, medizinische Zweckbestimmung, Sicherheitskomponente nach MDR). Alle AI-Act-Pflichten greifen. Schritt 2 HU-RAC: Datenkategorien Gesundheitsdaten nach Art. 9 DSGVO (sehr hoch), Betroffenenkreis Patienten mit Gefährdungspotenzial (sehr hoch), KI-Hochrisiko (sehr hoch). HU-RAC 4, Level A, R1 oder R2. Schritt 3 DSGVO: Art. 9 einschlägig, besondere Rechtsgrundlage

(typisch Art. 9 Abs. 2 lit. h), DSFA zwingend. Schritt 4 HU-RAC-spezifisch: zusätzliche E-Min-Controls aus Kapitel 5.1 (EU/CH-Datenverarbeitung, AVV, DSFA-Dokumentation) und 5.4 (Hardware Root of Trust, HYOK-Optionen, Kundenseitiges HSM empfohlen). E-Plus-Controls wie Zero-Knowledge und unabhängiges Kryptografie-Audit als Roadmap-Elemente. Sektorrecht: MDR mit CE-Konformität und ggf. Benannter Stelle, MPBetreibV, SGB V.

Kontakt und Rückmeldung

Dieses Impulspapier ist als Einladung zum Gespräch gedacht. Rückmeldungen, Kritik, Erweiterungsvorschläge und Hinweise auf verwandte Arbeiten sind willkommen. Die Autorin prüft die Anregungen und wird das Papier bei Bedarf überarbeiten. Eine zweite Fassung ist denkbar, sobald hinreichend Resonanz eingegangen ist.

Humanide GmbH

– Ansprechpartner und Kontaktdaten hier ergänzen –

Zitation: Humanide GmbH (2026): HU-RAC – Ein Denkmodell zur Klassifikation smarter Robotiksysteme nach Datenhoheit und Datensicherheit. Impulspapier, Version 0.3.1, April 2026.