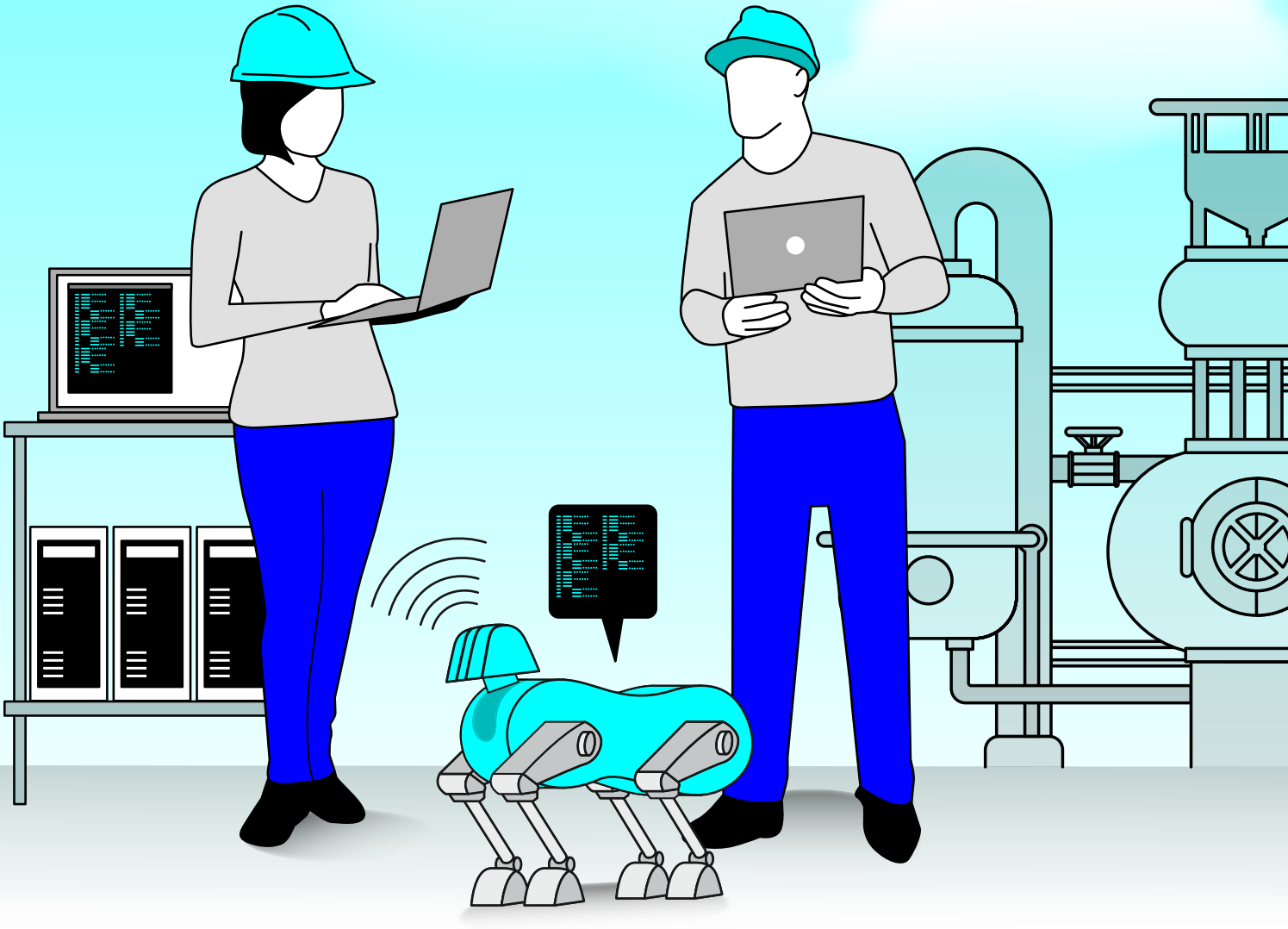
INNOVATION–SANDBOX
für Künstliche Intelligenz



Autonome Inspektionsroboter

Umgang mit der KI-Verordnung und dem EU-Maschinenrecht

innovationsandbox.ai

metropolitan konferenz zürich

Kanton Zürich

Innovation Zurich

Produktionsanlagen in Bereichen wie Energie, Öl, Gas, Nukleartechnologie oder Stromversorgung sind essenziell für Wirtschaft und Gesellschaft. Technische Ausfälle können gravierende Folgen haben – für Sicherheit, Umwelt und Versorgung. Regelmässige Inspektionen sind daher zentral, aber oft zeitintensiv und gefährlich. Zudem stehen immer weniger Fachkräfte dafür zur Verfügung. Autonome Inspektionsroboter bieten eine vielversprechende Lösung: Sie erfassen rund um die Uhr grosse Datenmengen, analysieren diese mittels künstlicher Intelligenz (KI) und übernehmen zahlreiche Aufgaben selbstständig. So lassen sich Fachkräfte entlasten, gefährliche Einsätze vermeiden und die Betriebssicherheit erhöhen. Die Nutzung solcher Systeme wirft jedoch komplexe Regulierungsfragen auf. Seit dem Inkrafttreten der EU-KI-Verordnung stehen viele Schweizer Robotikfirmen vor der Frage, wie sie diese Verordnung und weitere relevante EU-Vorgaben wie die Maschinenverordnung einhalten können. Im Rahmen der Innovation-Sandbox für KI haben das Amt für Wirtschaft des Kantons Zürich und das Center for Information Technology, Society, and Law (ITSL) der Universität Zürich basierend auf einem Anwendungsfall der Firma ANYbotics Strategien zum Umgang mit regulatorischen Vorgaben für autonome Inspektionssysteme entwickelt. Die Erkenntnisse sollen weitere Robotikunternehmen unterstützen und den Zugang zum EU-Markt erleichtern.

Innovation-Sandbox für KI

Das Projektteam hat das vorliegende Dokument im Rahmen der Innovation-Sandbox für KI erarbeitet. Die Sandbox ist eine Testumgebung für die Umsetzung von KI-Projekten aus verschiedenen Sektoren. Die breit abgestützte Initiative aus Verwaltung, Wirtschaft und Forschung fördert verantwortungsvolle Innovation, indem das Projektteam und teilnehmende Organisationen eng an regulatorischen Fragestellungen arbeiten und die Nutzung von neuartigen Datenquellen ermöglichen. Die Inhalte dieses Reports sind nicht rechtsverbindlich und stellen keine offizielle Position öffentlicher Organe dar. Jegliche Haftung für rechtliche Aspekte wird ausgeschlossen.

Mehr Informationen

Inhaltsverzeichnis

Mit fachlicher Unterstützung durch

Dr. Ann-Katrin Michel
Ressortleiterin Technik, Swissmem

Barbara Mullis
Normungsexpertin, Electrosuisse

Dr. Christian Gehring
Co-Founder and Sr. Director of Robotics & AI, ANYbotics

Dr. Clara Guerra
Stabsstellenleiterin, Stabsstelle für Digitale Innovation, Fürstentum Liechtenstein

Elena Maran
Global Head of Responsible AI, Modulos AG

Jonas Büchel
Juristischer Mitarbeiter, Wicki Partners AG

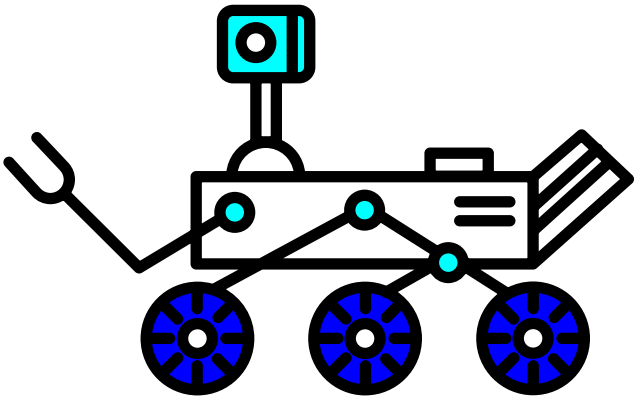
Kateryna Portmann
Senior Product Manager, ANYbotics

Kevin Schawinski
Co-Founder und CEO, Modulos AG

Marcel Fehr
Senior Certification Manager, ANYbotics

Yvonne Finger
Referatsleiterin, Bundesnetzagentur, Bundesrepublik Deutschland

01. *Potenziale autonomer Inspektionsroboter*



Industrieanlagen in Bereichen wie Energie, Öl und Gas, Stromversorgung oder Chemie zählen zu den komplexesten und sicherheitskritischsten Infrastrukturen unserer Gesellschaft. Ein einziger Ausfall kann weitreichende Konsequenzen haben – für die Versorgungssicherheit, die Umwelt oder das Personal vor Ort. Um Störungen vorzubeugen, sind regelmässige Inspektionen zwingend notwendig. Diese erfolgen in vielen Fällen manuell und analog: Mitarbeitende kontrollieren visuell, lesen Messgeräte ab oder dokumentieren Beobachtungen vor Ort. Eine systematische, kontinuierliche Datenerfassung findet kaum statt – und damit fehlt häufig die Grundlage für eine vorausschauende Wartung und präzise Fehleranalysen. Zugleich sind die Inspektionen sehr anspruchsvoll: Sie führen Personal in enge Räume, auf hohe Anlagen oder in explosionsgefährdete Zonen. Die körperliche Belastung ist hoch, und die Unfallgefahr ist real. Laut der Internationalen Arbeitsorganisation ereignen sich weltweit jährlich rund 395 Millionen nicht tödliche Arbeitsunfälle, wobei ein erheblicher Anteil auf gefährliche Industrieumgebungen zurückzuführen ist.[1] Hinzu kommt ein struktureller Fachkräftemangel: Viele Organisationen im Energiesektor haben Schwierigkeiten, ausreichend qualifiziertes Personal zu finden, um ihre Aktivitäten langfristig sicherzustellen.[2] Vor diesem Hintergrund gewinnen autonome Inspektionsroboter zunehmend an Bedeutung. Moderne Systeme können Anlagen rund um die Uhr überwachen, Daten erfassen und erste Auswertungen durchführen, ohne dass Menschen gefährdet werden. Diese Roboter basieren auf einem Zusammenspiel von Sensorik, KI, mobiler Robotik und ***digitalen Zwillingen***. Sie erfassen Temperatur, Schall, Lecks, visuelle Veränderungen oder Vibrationsmuster – und leiten daraus automatisiert Wartungsbedarf oder Gefahrenpotenzial ab. Viele dieser Systeme sind so konzipiert, dass sie mit Menschen zusammenarbeiten: Sie übernehmen Routinekontrollen, erfassen schwer zugängliche Stellen oder liefern dem Fachpersonal im Kontrollraum Echtzeitdaten. Dadurch wird die physische Präsenz von Menschen vor Ort reduziert und gleichzeitig die Entscheidungsqualität erhöht.

«Autonome Inspektionen werden künftig entscheidend für Sicherheit und Effizienz in der Industrie.» *Raphael von Thiessen, Programmleiter KI-Sandbox*

* Die blau markierten Begriffe sind auf Seite 37 im Glossar erklärt

[1] International Labour Organization (ILO), Occupational Safety and Health (Link).

[2] International Energy Agency, World Energy Employment 2023 (Link).

01. Potenziale autonomer Inspektionsroboter

Zentrale Mehrwerte autonomer Inspektionsroboter:

- **Sicherheitsgewinn**
  Menschen werden aus gefährlichen Situationen herausgehalten.

- **Bessere Datenbasis**
  Die kontinuierliche, standardisierte Erfassung und Übertragung verbessert die Daten.

- **Effizienzsteigerung**
  Automatisierte Routineaufgaben entlasten Personal und reduzieren Stillstandzeiten.

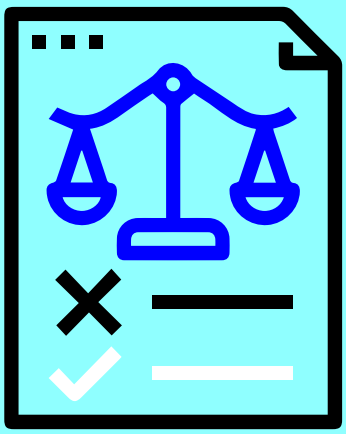
- **Entlastung von Fachkräften**
  Personalengpässe werden entschärft, da weniger Vor-Ort-Einsätze notwendig sind.

- **Zukunftsfähigkeit**
  Die Integration in digitale Systeme und Zwillinge schafft neue Automatisierungspotenziale.

Trotz dieser Vorteile bestehen auch Herausforderungen: Autonome Systeme können fehlerhafte Daten erfassen oder Auswertungen falsch interpretieren – insbesondere bei komplexen Umgebungsbedingungen oder unklaren Sensorwerten. Auch Fehlfunktionen in der Fortbewegung oder unerwartete Interaktionen mit dem Personal können Sicherheitsrisiken bergen – insbesondere in schwer navigierbaren Umgebungen. Um das volle Potenzial dieser Technologien auszuschöpfen, braucht es deshalb technische und organisationale Sicherheitskonzepte, eine laufende Qualitätssicherung und eine klare Verantwortungsteilung zwischen Mensch und Maschine.

Hinzu kommen neue regulatorische Fragestellungen: Während der rechtliche Rahmen für Maschinen – etwa im Bereich der Produktsicherheit – in der EU seit Jahren etabliert ist, bringt der KI-Einsatz neue Unsicherheiten mit sich. KI-Systeme, die selbstständig Entscheidungen treffen oder Risiken erkennen sollen, werfen Fragen der Transparenz, der Rechenschaftspflicht und der Haftung auf. Mit der *KI-Verordnung (AI Act)* besteht nun erstmals ein spezifischer Regulierungsrahmen für KI in der EU, doch dessen Zusammenspiel mit bestehenden EU-Vorschriften wie der *Maschinenrichtlinie (Machinery Directive)* bzw. der *Maschinenverordnung (Machinery Regulation)*, der *Datenverordnung (Data Act)* oder der *Cyberresilienzverordnung (Cyber Resilience Act)* stellt Hersteller und Betreiber vor zusätzliche Herausforderungen. Insbesondere bei Systemen, die sowohl als Maschine als auch als KI-Anwendung gelten, ist eine sorgfältige Abgrenzung und Kombination der regulatorischen Anforderungen notwendig.

02.
Relevante EU-Regulierungen



Seit dem Markteintritt autonomer Inspektionssysteme für sicherheitskritische Infrastrukturen wie Energie-, Industrie- oder Transportanlagen stellen sich für Schweizer Robotikhersteller zunehmend komplexe regulatorische Fragen. EU-Rechtsakte wie die KI-, die Maschinen-, die Daten- oder die Cyberresilienzverordnung schaffen neue Rahmenbedingungen, deren Anforderungen sich nicht nur überschneiden, sondern sich auch gegenseitig ergänzen oder in Spannung zueinanderstehen. Besonders betroffen sind Systeme mit integrierten KI-Komponenten – also Maschinen, die nicht nur mechanische Aufgaben ausführen, sondern datenbasiert analysieren, bewerten oder Entscheidungen vorbereiten bzw. fällen.

Das vorliegende Kapitel bietet eine strukturierte Einführung in die EU-Regulierungen, die für solche Systeme relevant sind. Ziel ist es, die regulatorischen Grundlagen kompakt darzustellen, Orientierung zu geben und Strategien für die rechtliche Einordnung und Umsetzung bereitzustellen – insbesondere für Hersteller mit Sitz in der Schweiz, die ihre Produkte in der EU vermarkten möchten.

Kapitel 3 vertieft diese Grundlagen anhand eines konkreten Praxisbeispiels aus der Innovation-Sandbox für KI des Kantons Zürich. Dort wurde der Einsatz von ANYmal, einem vierbeinigen Inspektionsroboter der Firma ANYbotics, genutzt, um zentrale regulatorische Fragen im Zusammenspiel von KI und Robotik systematisch zu bearbeiten. Die dabei entwickelten Handlungsoptionen und strategischen Überlegungen sind nicht nur für ANYbotics von Bedeutung, sondern haben auch hohe Praxisrelevanz für andere Robotikunternehmen in der Schweiz, die vergleichbare Systeme entwickeln oder vertreiben.

2.1 EU-Maschinenrichtlinie und -Maschinenverordnung

Inspektionsroboter dürften in den meisten Fällen unabhängig von ihrem Autonomiegrad als Maschinen zu qualifizieren sein und den dafür vorgesehenen gesetzlichen Vorgaben unterliegen. Einschlägig ist hier die schweizerische Maschinenverordnung, die auf der EU-Maschinenrichtlinie (EG-RL 2006/42/EG) basiert und deren Vorgaben ins Schweizer Recht umsetzt.

Was müssen Maschinenhersteller heute beachten, wenn sie Maschinen in der EU auf den Markt bringen möchten?

Wenn Hersteller einen Inspektionsroboter zusätzlich in der EU auf den Markt bringen wollen, müssen sie die Vorschriften der EU-Maschinenrichtlinie erfüllen. Erforderlich ist eine *Konformitätsbewertung*, in der sie erklären, dass die Maschine allen einschlägigen Anforderungen entspricht. Danach ist das CE-Kennzeichen als Nachweis der Konformität mit allen einschlägigen gesetzlichen Vorgaben anzubringen. Die Schweiz hat mit der EU ein bilaterales Abkommen über die gegenseitige Anerkennung von

02. Relevante EU-Regulierungen

Konformitätsbewertungen (Mutual Recognition Agreement [MRA]) abgeschlossen. Ziel des MRA war, eine einheitliche Konformitätsbewertung in der Schweiz oder der EU zu ermöglichen und die gegenseitige Anerkennung solcher Bewertungen sicherzustellen, d.h., dass eine Schweizer Konformitätsbewertungsstelle die EU-Konformität bescheinigen kann (und umgekehrt). Jedoch wurde das MRA seit der Ablehnung des Rahmenabkommens durch die Schweiz nicht mehr aktualisiert. Das bedeutet: Wenn eine im MRA enthaltene Regelung geändert oder ersetzt wird, fällt sie aus dem Anwendungsbereich des Abkommens heraus. Damit entfällt auch die gegenseitige Anerkennung der Gleichwertigkeit. Zurzeit ist die EU-Maschinenrichtlinie Teil des MRA und Schweizer Maschinenhersteller profitieren noch von der gegenseitigen Konformitätsanerkennung. Am 20. Januar 2027 wird die EU-Maschinenrichtlinie jedoch durch die neue EU-Maschinenverordnung ersetzt. Wenn das MRA bis dahin nicht aktualisiert wird, gilt die gegenseitige Anerkennung nicht mehr. Dann müssen Schweizer Hersteller die Konformitätsbewertung durch eine *notifizierte Stelle* in der EU durchführen lassen.

Ab wann ist die EU-Maschinenverordnung anwendbar?

Die neue EU-Maschinenverordnung (EU 2023/1230) wurde am 29. Juni 2023 im EU-Amtsblatt veröffentlicht und ist am 19. Juli 2023 formell in Kraft getreten. Ab dem 20. Januar 2027 ist sie anwendbar. Dann ersetzt sie die bisher geltende Maschinenrichtlinie 2006/42/EG. Als Verordnung ist sie – anders als eine Richtlinie – unmittelbar in allen Mitgliedstaaten anwendbar und bedarf keiner nationalen Umsetzung.

Bis zum 19. Januar 2027 bleibt die bisherige EU-Maschinenrichtlinie vollständig anwendbar. Hersteller dürfen aber bereits heute nach der neuen Verordnung arbeiten. Für eine rechtskonforme Inverkehrbringung müssen sie jedoch sicherstellen, dass die Anforderungen der alten Richtlinie nach wie vor erfüllt sind. Je nach Zeitpunkt des Inverkehrbringens muss ein Produkt die Anforderungen der EU-Maschinenrichtlinie bzw. die der EU-Maschinenverordnung erfüllen. Ist dieser Zeitpunkt unbekannt, sollte das Produkt beiden Regelwerken entsprechen. In diesem Fall kann eine doppelte Konformitätserklärung eine Lösung darstellen. Damit bestätigt der Hersteller, dass sein Produkt bei Inverkehrbringen bis zum 19. Januar 2027 der EU-Maschinenrichtlinie bzw. bei Inverkehrbringen ab dem 20. Januar 2027 der EU-Maschinenverordnung entspricht.

Ab dem 20. Januar 2027 ist die neue EU-Maschinenverordnung verbindlich. Dann dürfen Maschinen nur noch auf ihrer Grundlage in Verkehr gebracht werden. Nach EU-Recht bedeutet Inverkehrbringen die erstmalige Abgabe des Produkts zum Vertrieb oder zur Verwendung. Das Herstellungsdatum ist rechtlich irrelevant.

Maschinen, die vor dem 20. Januar 2027 nach der EU-Maschinenrichtlinie in Verkehr gebracht wurden, dürfen weiter genutzt, gehandelt und betrieben werden. Allein aufgrund der neuen Verordnung ist keine Nachrüstung erforderlich. Wenn eine bereits in Verkehr gebrachte Maschine aber wesentlich verändert wird (bspw. durch einen Umbau, einen Steuerungsersatz oder eine starke Veränderung der Funktionsweise), kann dies als neues Inverkehrbringen gelten.

Was ändert sich für autonome Inspektionsroboter mit der EU-Maschinenverordnung?

Die EU-Maschinenverordnung bringt wesentliche Neuerungen für Hersteller von autonomen Inspektionsrobotern. Wie weitreichend sie sind, beurteilt sich danach, welche Teile des Inspektionsroboters autonom sind. Die Verordnung enthält eine Definition für autonome mobile Maschinen.

02. Relevante EU-Regulierungen

Relevant sind insbesondere die neuen Vorschriften zu den Konformitätsbewertungen: Bei gewissen Maschinen können die Bewertungen nicht mehr durch den Hersteller selbst durchgeführt werden, d.h., eine Selbstdeklaration oder eine ***interne Fertigungskontrolle*** ist nicht mehr möglich. Dies betrifft Maschinen, die in Anhang I Teil A der EU-Maschinenverordnung aufgelistet sind. Darunter fallen nach Anhang I Teil A Ziffer 6 «Maschinen, die über eingebettete Systeme mit vollständig oder teilweise selbstentwickelndem Verhalten unter Verwendung von Ansätzen des maschinellen Lernens verfügen, die Sicherheitsfunktionen gewährleisten, die nicht gesondert in Verkehr gebracht wurden, nur in Bezug auf diese Systeme». Relevant sind die Neuerungen somit vor allem für KI-Komponenten, die Sicherheitsfunktionen gewährleisten.

Im Fall eines autonomen Inspektionsroboters dürfte die Definition aus Anhang I Teil A Ziffer 6 der EU-Maschinenverordnung in der Regel erfüllt sein, da maschinelles Lernen typischerweise für sicherheitsrelevante Navigations- und Hinderniserkennungsfunktionen eingesetzt wird, etwa um Kollisionen in komplexen Industrieumgebungen zu vermeiden – Funktionen, die unmittelbaren Einfluss auf den sicheren Betrieb des Roboters haben.

Die EU-Maschinenverordnung verlangt zudem explizit, dass die Maschine auch im Fall eines rechtmässigen oder unrechtmässigen Zugriffs nicht gefährlich wird (sog. Schutz vor Korrumpierung, Anhang III Teil B Ziffer 1.1.9).

Ausserdem werden zusätzlich zu den anderen möglicherweise anwendbaren grundlegenden Sicherheits- und Gesundheitsschutzanforderungen des Anhangs III noch separate Anforderungen hinsichtlich der Überwachungsfunktion aufgestellt (Anhang III Teil B Ziffer 3.2.4).

Was bedeutet das für die bisherigen Konformitätsbewertungen?
Vor dem 20. Januar 2027 nach der EU-Maschinenrichtlinie korrekt in Verkehr gebrachte Maschinen gelten weiterhin als rechtskonform. Ihre Konformitätserklärungen behalten ihre Rechtswirkung, auch über den Stichtag hinaus. Nach dem Stichtag dürfen Maschinen nicht mehr auf Grundlage der EU-Maschinenrichtlinie in Verkehr gebracht werden. Es ist zwingend die neue EU-Maschinenverordnung anzuwenden, und eine entsprechende EU-Konformitätserklärung ist erforderlich.

Welche Konformitätsbewertungsverfahren kommen infrage?
Für Maschinen, die in Anhang I Teil A der EU-Maschinenverordnung aufgeführt sind, ist ein Konformitätsbewertungsverfahren durch eine notifizierte Stelle (also nicht durch den Hersteller selbst) zwingend. Die Verordnung listet verschiedene mögliche Konformitätsbewertungsverfahren auf:

- **EU-Baumusterprüfung**
  Die notifizierte Stelle prüft ein Muster der Maschine und bewertet jeden einzelnen Maschinentyp.

- **Umfassende Qualitätssicherung**
  Nicht das Produkt, sondern das Qualitätssicherungssystem des Herstellers wird bewertet. Weil die Qualitätssicherung gewährleistet ist, erübrigt sich eine Bewertung der einzelnen Produkte.

- **Einzelprüfung**
  Jedes einzelne Produkt wird einer Bewertung unterzogen.

02. Relevante EU-Regulierungen

	EU-Baumusterprüfung	Umfassende Qualitätssicherung	Einzelprüfung
Vorteile	▪ Klare Prüfbarkeit eines repräsentativen Robotermodells ▪ Hohe Rechtssicherheit durch externe Bewertung ▪ Für Einzelsysteme mit stabiler Konfiguration geeignet ▪ Keine Dokumentation des Qualitätssicherungssystems erforderlich	▪ Nicht jeder Robotertyp muss bewertet werden ▪ Geeignet für Hersteller mit laufender Serienproduktion ▪ Flexibel bei Software- oder Modellanpassungen innerhalb definierter Prozesse	▪ Geeignet für Einzelfertigungen oder hoch spezialisierte Roboter ▪ Keine aufwendige Prüfung der Maschine vor Ort, da die Zertifizierung aufgrund von Dokumentationen erfolgt
Nachteile	▪ Jede wesentliche Modelländerung erfordert eine neue Prüfung ▪ Hersteller muss der notifizierten Stelle Zugang zur Maschine gewähren ▪ Langwierig bei häufigen Updates (z.B. bei KI-Weiterentwicklungen) ▪ Eingeschränkte Flexibilität bei Softwareanpassungen	▪ Grösserer Initialaufwand ▪ Aufwendigere interne Prozesse und umfangreiche Dokumentation erforderlich ▪ Mögliche unangemeldete Audits ▪ Für kleinere Anbieter unter Umständen wirtschaftlich weniger attraktiv	▪ Aufwendigere interne Prozesse und umfangreiche Dokumentation (auch des Qualitätssicherungssystems) erforderlich ▪ Für kleinere Anbieter unter Umständen wirtschaftlich weniger attraktiv

Für autonome Inspektionsroboter mit sicherheitsrelevanter KI ist bei stabilen Systemen meist die EU-Baumusterprüfung sinnvoll (siehe dazu Kapitel 3.2). Bei Serienproduktion eignet sich die Qualitätssicherung, während die Einzelprüfung nur für wenige, individuell konfigurierte Roboter praktikabel ist.

Wie sieht das Konformitätsverfahren für autonome Inspektionsroboter aus?
Wenn KI-Bestandteile des Inspektionsroboters unter Anhang I Teil A fallen, muss der Hersteller die Konformitätsbewertung von einer notifizierten Stelle durchführen lassen, bevor er die CE-Kennzeichnung anbringen darf. Dazu muss er eine umfassende technische Dokumentation bereitstellen, inklusive Unterlagen zur Risikobewertung und zu Sicherheitsnachweisen der KI-Komponente sowie Informationen zur Trainings- und Validierungsumgebung. Je nach gewähltem Verfahren (z.B. EU-Baumusterprüfung oder Qualitätssicherung) ist mit einem Aufwand von mehreren Wochen bis Monaten und entsprechenden Kosten zu rechnen – insbesondere für Prüfverfahren, Audits und Dokumentationsaufbereitung. Eine enge Abstimmung mit der notifizierten Stelle ist dabei entscheidend.

Handlungsempfehlungen

Für Hersteller von autonomen Inspektionsrobotern empfehlen sich die folgenden Schritte:

- **Einstufung nach Anhang I Teil A prüfen**
  frühzeitig klären, ob sicherheitsrelevante KI-Funktionen des Roboters unter den Anhang I Teil A Ziffer 6 der EU-Maschinenverordnung fallen.
- **Übergangsfrist nutzen**
  bis zum 19. Januar 2027 interne Umstellungen und Produktanpassungen vornehmen.
- **Konformitätsbewertungsverfahren wählen**
  in Abstimmung mit einer notifizierten Stelle prüfen, welches Verfahren geeignet ist.
- **Notifizierte Stelle einbinden**
  wenn sicherheitsrelevante KI-Komponenten vorliegen und eine externe Konformitätsbewertung somit zwingend ist, eine notifizierte Stelle kontaktieren.
- **Technische Dokumentation vorbereiten**
  Vollständigkeit der Unterlagen sicherstellen – inklusive Unterlagen zur Risikobewertung und zu Sicherheitsnachweisen für KI-Komponenten sowie Informationen zur Trainings- und Validierungsumgebung.
- **Cybersecurity-Anforderungen beachten**
  verpflichtende Vorgaben zum Schutz vor Cyberangriffen und zur sicheren Softwareverwaltung berücksichtigen.
- **Verzahnung mit der KI-Verordnung mitdenken**
  Schnittstellen zur KI-Verordnung beachten – insbesondere bei sicherheitsrelevanten, lernenden Systemen (siehe Kapitel 2.2).

2.2. EU-KI-Verordnung

Die EU-KI-Verordnung regelt die Entwicklung, den Vertrieb und die Nutzung von KI-Systemen und -Anwendungen im EU-Binnenmarkt und folgt einem risikobasierten Ansatz. Sie unterscheidet zwischen inakzeptablen und damit verbotenen, hoch riskanten, risikoarmen und minimal riskanten KI-Systemen. Kernstück der Verordnung sind detaillierte Vorschriften, die von Herstellern, Betreibern und sonstigen Beteiligten der KI-Wertschöpfungsketten befolgt werden müssen.

Welche Vorschriften gelten für Hochrisikosysteme?

Für Hochrisiko-KI-Systeme gelten nach der EU-KI-Verordnung strenge gesetzliche Anforderungen, da sie potenziell erhebliche Auswirkungen auf die Sicherheit, die Gesundheit oder die Grundrechte der EU-Bürgerinnen und -Bürger haben können. Die wesentlichen Pflichten finden sich in den Artikeln 8–20 der EU-KI-Verordnung. Besondere Vorschriften gibt es bspw. bezüglich des Risikomanagementsystems. So besteht die Pflicht, einen kontinuierlichen Risikomanagementprozess zur Erkennung, Minimierung und Überwachung von Risiken über den gesamten Lebenszyklus der Systeme durchzuführen und zu dokumentieren. Auch an die Datenqualität werden Anforderungen gestellt: Die Trainings-, Validierungs- und Testdaten müssen relevant, repräsentativ, fehlerfrei und diskriminierungsfrei sein. Weitere Pflichten betreffen u.a. die technische Dokumentation, die Protokollierungsfunktion, die Transparenz und die menschliche Aufsicht.

Für wen gelten die Vorschriften der EU-KI-Verordnung?

Die EU-KI-Verordnung erfasst fast alle Beteiligten entlang der Wertschöpfungskette eines KI-Systems, das in der EU auf den Markt gebracht oder dessen Output bestimmungsgemäss in der EU verwendet werden soll. Dazu gehören auch Unternehmen, die ihren Sitz nicht in der EU haben. Es gilt das Marktortprinzip. Dies betrifft namentlich Hersteller, Anbieter und Betreiber aus einem Drittland wie der Schweiz.

Ab wann kommen die Vorschriften der EU-KI-Verordnung zur Anwendung, und welche Übergangsfristen gelten?

Der Gesetzgeber hat ein zeitlich gestuftes Regime für das Inkrafttreten der EU-KI-Verordnung sowie Übergangsvorschriften für bereits auf dem Markt befindliche Systeme vorgesehen. Einzelne Vorgaben, bspw. das Verbot bestimmter KI-Praktiken (Art. 5), sind bereits am 2. Februar 2025 in Kraft getreten.

Am 2. August 2025 sind zusätzliche Anforderungen wirksam geworden: Transparenzpflichten für *General-Purpose AI*, Meldepflichten und Sanktionen. Auch administrative Vorgaben wie Governance-Regeln sind zu diesem Zeitpunkt in Kraft getreten. Das allgemeine Inkrafttreten der meisten Vorgaben, insbesondere für Hochrisiko-KI-Systeme, erfolgt am 2. August 2026. Für die strengsten Pflichten bei Hochrisiko-KI gilt eine Übergangsfrist bis 2. August 2027.

Welche Stichtage sind für autonome Inspektionsroboter besonders relevant?

Weil autonome Inspektionsroboter in vielen Fällen als Hochrisikosysteme qualifiziert werden dürften, sind für sie die Vorschriften für diese Systeme besonders relevant. Die EU-KI-Verordnung enthält in Artikel 111 Übergangsfristen für bereits auf dem Markt befindliche Hochrisikosysteme. Hochrisikosysteme, die vor dem 2. August 2026 in Verkehr gebracht und nicht wesentlich verändert werden, unterliegen nicht der EU-KI-Verordnung. Für Hochrisikosysteme, die in Behörden verwendet werden, gilt eine Übergangsfrist bis 2. August 2030. Die Fris-

ten gelten nicht für verbotene Systeme (siehe weiter unten).

Was gilt als wesentliche Veränderung bei autonomen Inspektionsrobotern?
Damit Hochrisikosysteme nicht von der EU-KI-Verordnung erfasst werden, müssen sie vor dem 2. August 2026 in Verkehr gebracht oder in Betrieb genommen werden und dürfen danach in ihrer Konzeption nicht mehr wesentlich verändert werden. Wann eine wesentliche Veränderung vorliegt, wird in Artikel 3 Absatz 23 und EG 128 der EU-KI-Verordnung näher definiert. Als wesentlich gelten Veränderungen, die bei der ursprünglichen Konformitätsbewertung vom Anbieter nicht vorgesehen oder geplant waren und die Konformität beeinträchtigen oder zu einer Veränderung der Zweckbestimmung führen, für die das KI-System bewertet wurde. Bereits Änderungen des Betriebssystems oder der Softwarearchitektur stellen gemäss der Verordnung eine wesentliche Zweckveränderung dar, nicht jedoch Änderungen im Algorithmus und in der Leistung, wenn diese automatisch während des Betriebs erfolgen und wenn diese Anpassungsfähigkeit vom Anbieter vorgesehen und im Rahmen der Konformitätsbewertung berücksichtigt wurde. In der Praxis wird sich noch zeigen, wie diese Vorgaben im Detail interpretiert werden. Folgt man jedoch dieser breiten Auslegung, kann praktisch jeder Eingriff in das KI-System zu einer wesentlichen Veränderung führen.

Da es um Produktsicherheitsrecht geht, wäre es auch denkbar, zur Auslegung der EU-KI-Verordnung die Vorschriften der EU-Produktsicherheitsverordnung beizuziehen. Nach Artikel 13 Absatz 3 dieser Verordnung ist die Veränderung eines Produkts nur dann wesentlich, wenn sie sich (1) auf die Produktsicherheit auswirkt, (2) nicht in der ursprünglichen Risikobewertung berücksichtigt war, (3) eine neue oder geänderte Gefahr mit sich bringt und (4) nicht durch den Verbraucher selbst erfolgt ist. Relevant ist somit, ob die Veränderung mit der Erhöhung der Gefahren oder der Risiken einhergeht. In diesem Sinne könnte man argumentieren, dass Routineänderungen (z.B. Betriebssystemupdates), die das Risiko nicht erhöhen, oder Änderungen, die das Risiko gar vermindern, keine wesentlichen Veränderungen darstellen. Es ist jedoch davon auszugehen, dass die Behörden einen eher strengen Massstab anlegen und einen grossen Teil der KI-Systeme von der KI-Verordnung erfasst haben möchten.

Gibt es weitere Ausnahmen von der Anwendung der EU-KI-Verordnung?
In gewissen Bereichen gilt die Verordnung nur sehr eingeschränkt oder gar nicht. Dies betrifft einige wesentliche Wirtschaftssektoren wie die Zivilluftfahrt, die Land- und die Forstwirtschaft, die Schiffausrüstung oder den Automobilbereich inklusive des autonomen Fahrens. Für diese Bereiche existieren bereits spezifische Zulassungsregulierungen. Ebenfalls von der Verordnung ausgenommen sind bestimmte Systeme, die einen militärischen Zweck erfüllen oder im Zusammenhang mit der internationalen Strafverfolgung stehen, sowie Systeme, die allein der wissenschaftlichen Forschung und Entwicklung dienen, inklusive sämtlicher damit verbundener Tätigkeiten. Auch Systeme, die natürliche Personen bei persönlichen Tätigkeiten unterstützen oder unter freier und quelloffener Lizenz stehen, sind ausgenommen, sofern sie nicht verboten sind oder besonderen Transparenzpflichten unterliegen. Die Anwendung der KI-Verordnung entfällt auch, wenn der persönliche Anwendungsbereich nicht erfüllt ist. Namentlich kann ein Anbieter seine Anbieterrolle verlieren, wenn etwa ein Händler, Einführer oder Betreiber das bereits in der EU in Verkehr gebrachte oder in Betrieb genommene KI-System mit seinem Namen oder seiner Handelsmarke ver-

sieht oder wesentliche Änderungen am System vornimmt. Dies kann bspw. durch einen sogenannten «White Label»-Verkauf geschehen. Denkbar ist auch, dass ein Anbieter das in der Schweiz produzierte KI-System einer Rechtseinheit in der EU zur Inverkehrsetzung überlässt.

Gibt es Erleichterungen für kleinere Hersteller von autonomen Inspektionsrobotern?
Ja, kleine und mittlere Unternehmen (KMU) sowie Start-ups mit Sitz oder Zweitniederlassung in der EU, die weniger als 250 Personen beschäftigen oder entweder einen Jahresumsatz von max. 50 Mio. Euro oder eine Jahresbilanzsumme von max. 43 Mio. Euro aufweisen, profitieren von gewissen Erleichterungen. Sie müssen bspw. eine weniger umfangreiche technische Dokumentation bereitstellen und niedrigere Gebühren für die Konformitätsbewertung entrichten. Zudem soll ihnen ein vorrangiger und kostenloser Zugang zu *KI-Reallaboren* gewährt werden. Auch bei der Sanktionszumessung spielt die Grösse des Unternehmens eine Rolle. Hinsichtlich der Mitarbeiterschulungen und des Risikomanagements gelten für KMU aber die gleichen Vorgaben wie für grössere Unternehmen.

Handelt es sich bei einem autonomen Inspektionsroboter immer um ein Hochrisikosystem?
Die EU-KI-Verordnung sieht zwei verschiedene Kategorien von Hochrisikosystemen vor. Nach Artikel 6 Absatz 1 gilt ein KI-System als hoch riskant, wenn die beiden Bedingungen a) und b) erfüllt sind: a) Das KI-System ist selbst ein Produkt, das unter die in Anhang I aufgeführten EU-Rechtsvorschriften fällt, oder es wird als Sicherheitsbauteil eines Produkts (z.B. als KI-Sicherheitsbauteil in Maschinen) verwendet, das unter die in Anhang I aufgeführten EU-Rechtsvorschriften fällt, und b) nach dem EU-Harmonisierungsrechtsakt ist eine Konformitätsbewertung durch Dritte erforderlich, bevor das Produkt auf den EU-Markt eingeführt wird. Zu den Harmonisierungsrechtsakten zählen bspw. die Maschinenverordnung, die Medizinprodukteverordnung, die Spielzeugsicherheitsrichtlinie oder die Fahrzeugsicherheitsvorschriften. Die relevanten Rechtsakte finden sich in Anhang I zur KI-Verordnung.

Als Harmonisierungsrechtsakt kommt für autonome Inspektionsroboter die EU-Maschinenrichtlinie (bzw. zum relevanten Zeitpunkt die EU-Maschinenverordnung) in Betracht. Wenn der autonome Inspektionsroboter ein Sicherheitsbauteil mit KI verwendet oder selbst ein Sicherheitsbauteil ist (was nicht der Fall sein dürfte), gilt er als Hochrisikosystem, wenn die EU-Maschinenverordnung eine Konformitätsbewertung vorsieht (siehe Kapitel 2.1).

Ein Sicherheitsbauteil ist nach Artikel 3 Ziffer 14 der EU-KI-Verordnung ein Bestandteil eines Produkts oder KI-Systems, der eine Sicherheitsfunktion für dieses Produkt oder KI-System erfüllt oder dessen Ausfall oder Störung die Gesundheit und Sicherheit von Personen oder Eigentum gefährdet. Im autonomen Inspektionsroboter befindet sich das KI-System häufig im Steuerungsbereich. Es ist deshalb davon auszugehen, dass sein Ausfall zumindest Eigentum gefährden könnte. Somit ist Bedingung a) erfüllt. Zudem muss das Gesamtprodukt, d.h. der Roboter, gemäss EU-Maschinenverordnung eine Konformitätsbewertung durchlaufen. Damit ist auch Bedingung b) erfüllt. Es ist also sehr wahrscheinlich, dass ein Inspektionsroboter als Hochrisikosystem im Sinne von Artikel 6 Absatz 1 der EU-KI-Verordnung qualifiziert wird. Je nachdem, welche Funktionen das KI-System genau wahrnimmt, kann dies aber auch nicht der Fall sein.

Darüber hinaus werden auch alle in Anhang III der Verordnung genannten Systeme als hoch riskant

eingestuft. Dies, weil sie in sicherheitskritischen Bereichen eingesetzt werden. Dazu zählen unter anderem kritische Infrastrukturen. Gemäss Anhang III Ziffer 2 gelten im Zusammenhang mit kritischen Infrastrukturen nur KI-Systeme als hoch riskant, die bestimmungsgemäss als Sicherheitsbauteile im Rahmen der Verwaltung und des Betriebs kritischer digitaler Infrastruktur, des Strassenverkehrs oder der Wasser-, Gas-, Wärme- oder Stromversorgung verwendet werden sollen. Deshalb ist wiederum entscheidend, ob es sich beim KI-System um ein Sicherheitsbauteil handelt.

In diesem Zusammenhang stellt sich die Frage, ob das KI-System bzw. der autonome Roboter als Sicherheitsbauteil der kritischen Infrastruktur qualifiziert werden kann. Wiederum ist massgeblich, ob ein Ausfall des Systems das Risiko für die Sicherheit oder Gesundheit von Menschen erhöht. Bei autonomen Inspektionsrobotern, die lediglich zur Datenerfassung dienen (z.B. zur visuellen Kontrolle oder Zustandserfassung), ohne direkt in Steuerungs- oder Betriebsprozesse einzugreifen, liegt in der Regel kein Sicherheitsbauteil im Sinne der KI-Verordnung vor. Entsprechend fällt das System auch nicht automatisch in die Hochrisikokategorie nach Anhang III Ziffer 2 der EU-KI-Verordnung. Anders verhält es sich bei KI-Systemen, die aktiv sicherheitsrelevante Funktionen übernehmen – etwa eine KI, die Stromflüsse in einem Energieversorgungssystem steuert. Hier liegt klar ein Sicherheitsbauteil vor, was eine entsprechende Konformitätsbewertung durch eine notifizierte Stelle erforderlich macht. Eine genaue Prüfung der Systemfunktion und -verwendung ist daher essenziell.

Gibt es weitere Ausnahmen von der Anwendung der KI-Verordnung?
Die Anwendung der KI-Verordnung entfällt auch, wenn der persönliche Anwendungsbereich nicht erfüllt ist. Namentlich kann ein Anbieter seine Anbieterrolle verlieren, wenn etwa ein Händler, Einführer oder Betreiber das bereits in der EU in Verkehr gebrachte oder in Betrieb genommene KI-System mit seinem Namen oder seiner Handelsmarke versieht oder wesentliche Änderungen am System vornimmt. Dies kann bspw. durch einen sogenannten «White Label»-Verkauf geschehen. Denkbar ist auch, dass ein Anbieter das in der Schweiz produzierte KI-System einer Rechtseinheit in der EU zur Inverkehrsetzung überlässt.

Konformitätsbewertungen nach EU-Maschinen- und EU-KI-Verordnung

Wann sind gemäss EU-KI-Verordnung Konformitätsbewertungen vorgesehen?
Konformitätsbewertungen sind nur für Hochrisiko-KI-Systeme vorgesehen. Sie sollen nachweisen, dass das System mit den Anforderungen der EU-KI-Verordnung übereinstimmt (z.B. hinsichtlich Datenqualität, Transparenz, Risikomanagement, menschlicher Aufsicht).

Wenn das Hochrisiko-KI-System Teil eines Produkts ist, das anderen EU-Harmonisierungsrechtsakten unterliegt (z.B. eines Medizinprodukts, einer Maschine oder eines Fahrzeugs), ist grundsätzlich eine externe Konformitätsbewertung durch eine notifizierte Stelle erforderlich. Diese prüft die Konformität und stellt gegebenenfalls eine EU-Konformitätserklärung aus. Wenn ein KI-System die Konformitätsbewertung erfolgreich durchläuft, darf es mit dem CE-Kennzeichen versehen werden (siehe Kapitel 2.1).

02. Relevante EU-Regulierungen

Inwiefern kann eine bestehende Konformitätsbewertung gemäss EU-Maschinenrichtlinie bzw. -verordnung angerechnet werden?
In der EU-KI-Verordnung ist an verschiedenen Stellen festgehalten, dass bei Produkten und KI-Systemen, die im Rahmen von Harmonisierungsrechtsvorschriften bereits gewisse Konformitätsbewertungen durchlaufen haben, die für diese Bewertungen verwendeten Unterlagen und Dokumentationen auch für die Dokumentation gemäss EU-KI-Verordnung verwendet werden können bzw. dass die Anforderungen der EU-KI-Verordnung in die bestehende Dokumentation integriert werden können.

Müssen zwei Konformitätsbewertungsverfahren durchgeführt werden, d.h. eine nach EU-Maschinenverordnung und eine nach EU-KI-Verordnung?
Nein, es werden wohl nicht zwei verschiedene Verfahren durchgeführt. Wenn ein Produkt unter die EU-Maschinenverordnung fällt, wird ein Konformitätsbewertungsverfahren dieser Verordnung angewendet. Da sich ihre Anforderungen in grossen Teilen mit denjenigen der EU-KI-Verordnung decken (siehe die Checkliste für Hochrisikosysteme in Kapitel 3.2), wird innerhalb dieses Verfahrens hauptsächlich die Einhaltung der EU-Maschinenverordnung geprüft. Falls es aber eine Anforderung der EU-KI-Verordnung gibt, die dadurch nicht abgedeckt wird, wird diese Anforderung im selben Verfahren durch dieselbe notifizierte Stelle geprüft.

Ist die gesamte Maschine einer Konformitätsbewertung durch eine notifizierte Stelle zu unterziehen oder nur Teile davon?
Es muss nicht der gesamte Roboter bzw. die gesamte Maschine durch die notifizierte Stelle bewertet werden, sondern nur die Teile, die eine Sicherheitsfunktion gewährleisten. Im Fall eines autonomen Inspektionsroboters dürfte das die Steuerungszentrale sein. Die restlichen Teile müssen durch den Hersteller selbst überprüft und einer Konformitätsbewertung unterzogen werden.

«Bei KI-basierten Robotiksystemen zeigt sich, wie komplex und umfangreich die Vorgaben des EU-Rechts sind.»
Stephanie Volz, Geschäftsführerin ITSL

Handlungsempfehlungen

- **Hochrisikoeinstufung prüfen**
  sorgfältig prüfen, ob das KI-System als Sicherheitsbauteil gemäss EU-Maschinenverordnung oder als Hochrisikosystem gemäss Anhang III der EU-KI-Verordnung einzustufen ist.
- **Übergangsfristen berücksichtigen**
  bei der Marktplanung bedenken, dass Systeme, die vor dem 2. August 2026 in Verkehr gebracht und nicht wesentlich verändert werden, nicht unter die neuen Pflichten der EU-KI-Verordnung fallen.
- **Systemänderungen beurteilen**
  bei Anpassungen an Software, Betriebssystem oder Systemarchitektur eine differenzierte Risikoabwägung vornehmen, denn sie können als wesentliche Veränderung gelten und eine neue Konformitätsbewertung erforderlich machen.
- **Konformitätsverfahren integrieren**
  die für Hochrisikosysteme erforderliche Konformitätsbewertung gemäss EU-KI-Verordnung mit der Bewertung gemäss EU-Maschinenverordnung kombinieren.
- **Bestehende Dokumentationen nutzen**
  zur Erfüllung der Anforderungen der EU-KI-Verordnung die technischen Unterlagen aus der Konformitätsbewertung nach EU-Maschinenverordnung verwenden.
- **Erleichterungen für KMU berücksichtigen**
  die administrativen Erleichterungen für KMU der EU-KI-Verordnung, unter anderem reduzierte Dokumentationspflichten und einen kostenfreien Zugang zu Reallaboren, in Anspruch nehmen.
- **Anbieterrolle regeln**
  die Rolle des Anbieters allenfalls auf eine Rechtseinheit mit Sitz in der EU übertragen und die regulatorischen Pflichten damit gezielt verlagern. Dies ist möglich, sofern keine verbotenen Umgehungstatbestände vorliegen.

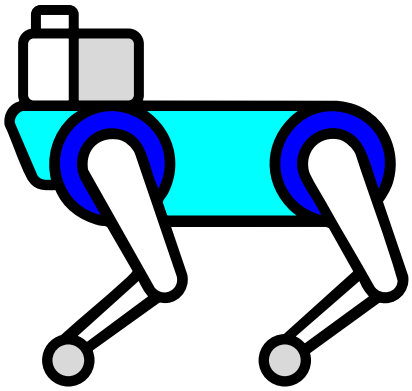
2.3. Weitere Rechtsakte

Neben den zentralen Regelwerken – **Maschinenverordnung und KI-Verordnung** – sind weitere regulatorische Entwicklungen auf EU-Ebene zu beachten, die ebenfalls Auswirkungen auf autonome Inspektionssysteme haben können:

- **Datenverordnung (Data Act)**
  Die Datenverordnung schafft einen einheitlichen Rechtsrahmen für die Nutzung, Weitergabe und den Zugang zu Daten in der EU. Sie verpflichtet Hersteller und Anbieter vernetzter Produkte sowie verbundener Dienstleistungen, generierte Daten zugänglich zu machen und regelt den Datenaustausch zwischen Unternehmen (B2B) und gegenüber öffentlichen Stellen (B2G). Für Betreiber autonomer Inspektionssysteme sind insbesondere die Anforderungen an Datenportabilität, Zugriffsrechte und vertragliche Transparenz relevant.

- **Cyberresilienzverordnung (Cyber Resilience Act)**
  Die Cyberresilienzverordnung führt horizontale Cybersicherheitsanforderungen für sämtliche digitale Produkte mit vernetzter Funktionalität ein. Hersteller müssen Sicherheits-by-Design und -by-Default nachweisen, Schwachstellenmanagement betreiben sowie Sicherheitsupdates während des gesamten Produktlebenszyklus gewährleisten. Für autonome Inspektionssysteme bedeutet dies erhöhte Anforderungen an sichere Softwareentwicklung, Patch-Management und den Nachweis entsprechender Prozesse im Rahmen der Konformitätsbewertung.

03. *Sandbox-Projekt mit ANYbotics*



3.1. Anwendungsfall ANYmal

Im Rahmen der Innovation Sandbox für KI diente das Produkt ANYmal als Anwendungsfall, um regulatorische Anforderungen zu klären. ANYmal ist ein autonomer, vierbeiniger Inspektionsroboter des Schweizer Unternehmens ANYbotics, entwickelt für anspruchsvolle Industrieumgebungen wie Energieanlagen, Offshore-Plattformen oder chemische Betriebe. Dank seiner dynamischen Laufmechanik kann er sich stabil über unebenes Gelände, Treppen und Gitterroste bewegen – überall dort, wo rad- oder kettenbasierte Systeme an ihre Grenzen stossen.

Die Plattform kombiniert drei integrierte KI-Komponenten, die meist lokal auf leistungsfähigen CPU/GPU-Einheiten verarbeitet werden:

- *Reinforcement Learning* **für Lokomotion**
  adaptive Fortbewegung in komplexen Umgebungen
- **Selbstlernende Navigation**
  autonome Wegfindung und Hindernisvermeidung
- *Supervised Learning* **für Inspektionen**
  Auswertung visueller, akustischer und physikalischer Sensordaten

ANYmal nutzt ein multimodales Sensorsystem, zu dem unter anderem folgende Komponenten gehören:

- **360°-***LIDAR* für eine *SLAM*-basierte Kartierung und Navigation
- **Tiefen- und Zoomkameras** für die visuelle Erkennung und Dokumentation
- **Wärmebildkamera** zur Temperaturüberwachung
- **Akustik-** und **Vibrationssensoren** zur Zustandsüberwachung von Maschinen

Die Kommunikation läuft typischerweise über WLAN, 5G oder Edge-Computing-Schnittstellen und ist direkt mit digitalen Zwillingen oder industriellen Überwachungssystemen verbunden. Die Energieversorgung erfolgt über eine automatische Ladestation, die einen kontinuierlichen Betrieb gewährleistet.

Kernfunktionen von ANYmal

- **Mobiles Mapping und 3D-Scanning**
  Erfassung ganzer Anlagen in hoher Auflösung
- **Sensorintegration**
  Temperatur, Leckage, visuelle Anzeigen (z.B. Füllstände, Manometer), Geräusche und Vibration
- **Intelligente Inspektion**
  automatische Anpassung der Sensorposition (z.B. Kamerawinkel bei Spiegelung), zusätzliche Aufnahmen bei Unklarheiten

03. Sandbox-Projekt mit ANYbotics

- **Echtzeitdatenübertragung**
  direkte Übermittlung der Informationen ins zentrale Überwachungssystem oder in den digitalen Zwilling der Anlage
- **Robustes Design**
  Schutz gegen Hitze, Staub, Feuchtigkeit, explosive Umgebungen (ATEX-zertifizierte Version verfügbar)

ANYmal wird heute weltweit in produktiven Umgebungen eingesetzt – von Energieversorgern bis hin zur chemischen Industrie. Der Roboter unterstützt bspw. bei Routinekontrollen, bei der präventiven Wartung oder bei Notfalleinsätzen.

Beispielanwendung 1: Chemieanlage
In einer chemischen Produktionsanlage wird der autonome Inspektionsroboter ANYmal im Regelbetrieb für tägliche Kontrollgänge eingesetzt. Er prüft über 120 visuelle, thermische und akustische Inspektionspunkte pro Mission, darunter Temperaturanzeigen, Pumpengeräusche und Korrosionsmerkmale. Abweichungen werden dokumentiert und automatisch gemeldet. Die dabei erfassten Daten fliessen in den digitalen Zwilling der Anlage ein und unterstützen eine kontinuierliche Zustandsüberwachung. Laut Betreiber konnte durch den Einsatz des Systems eine messbare Steigerung der Anlagenverfügbarkeit erreicht werden. Eine Ausweitung auf weitere Standorte ist vorgesehen.

Beispielanwendung 2: Offshore-Anlage
Auf einer Offshore-Anlage wird der autonome Inspektionsroboter ANYmal X im Rahmen regelmässiger Kontrollgänge eingesetzt. Er prüft visuelle, thermische und akustische Merkmale an Ventilen, Pumpen und elektrischen Anlagen – auch in explosionsgefährdeten Bereichen mit hoher Luftfeuchtigkeit und wechselnden Witterungsbedingungen. Die Inspektionen erfolgen auf mehreren Ebenen und in schwer zugänglichen Bereichen. Die dabei erfassten Daten werden automatisch an das Instandhaltungsteam übermittelt und in bestehende digitale Systeme integriert. Laut Betreiber leistet das System einen Beitrag zur Reduktion personeller Präsenz in sicherheitskritischen Zonen und zur kontinuierlichen Überwachung des Anlagenzustands.

03. Sandbox-Projekt mit ANYbotics

Beispielanwendung 3: Rechencenter
In einem Rechencenter wird der autonome Inspektionsroboter ANYmal für regelmässige Kontrollgänge eingesetzt. Er überwacht visuelle, thermische und akustische Zustandsmerkmale an gebäudetechnischen Anlagen wie Kühlung, Stromversorgung und Verkabelung – auch bei schlechten Lichtverhältnissen oder in der Nacht. Die Inspektionsdaten werden automatisch aufgezeichnet und an die betriebseigene Wartungsplattform übermittelt. Abweichungen werden erkannt und gemeldet, um frühzeitig manuelle Eingriffe zu ermöglichen. Laut Betreiber trägt der Einsatz des Systems zur Erhöhung der Betriebssicherheit und zur Automatisierung wiederkehrender Prüfaufgaben bei. Der Roboter ist dauerhaft im Einsatz und führt mehrere Inspektionsmissionen pro Tag durch.

Die drei Anwendungsbeispiele – Chemieanlage, Offshore-Plattform und Rechencenter – verdeutlichen die Bandbreite möglicher Einsatzbereiche autonomer Inspektionsrobotik in realen Industrieumgebungen. Sie zeigen, wie solche Systeme dazu beitragen können, bestehende Kontrollprozesse zu ergänzen, insbesondere in schwer zugänglichen oder sicherheitskritischen Bereichen. Gleichzeitig machen sie deutlich, welche technischen, organisatorischen und regulatorischen Fragen bei der Einführung solcher Technologien zu berücksichtigen sind.

Nutzen in der Praxis
- Verbesserte Inspektion, um Risiken und technische Probleme frühzeitig zu erkennen
- Reduktion von Personaleinsätzen in gefährlichen Zonen
- Basis für vorausschauende Wartung und langfristige Kostensenkung
- Lückenlose Dokumentation und verbesserte Datenqualität
- Entlastung von Fachpersonal bei repetitiven Kontrollaufgaben
- Integration in digitale Zwillinge und bestehende Monitoringsysteme

Herausforderungen in der Umsetzung
- Integration in bestehende Infrastrukturen und IT-Systeme
- Anpassung der Betriebsabläufe an robotergestützte Inspektionsprozesse
- Schulung von Personal für Betrieb und Wartung des Systems
- Anspruchsvolle Umweltbedingungen (z.B. extreme Hitze, Feuchtigkeit)
- Netzwerkverbindung für die Echtzeitdatenübertragung
- Kontinuierliche Systemkalibrierung und Fehlererkennung

03. Sandbox-Projekt mit ANYbotics

3.2. Umgang mit EU-Regulierungen

Die rechtliche Einordnung autonomer Inspektionsroboter stellt Hersteller und Regulierungsbehörden vor komplexe Herausforderungen. Insbesondere die Schnittstelle zwischen der EU-KI-Verordnung und der EU-Maschinenverordnung wirft zentrale Fragen auf: Unter welchen Voraussetzungen sind solche Systeme als Hochrisiko-KI-Systeme (HRKIS) einzustufen (siehe Kapitel 2.2)? Welche Pflichten ergeben sich daraus für die Hersteller, und welche Möglichkeiten entstehen durch verschiedene Auslegungen? Das folgende Kapitel analysiert am Beispiel des Roboters ANYmal (siehe Kapitel 3.1) mögliche Strategien im Umgang mit den regulatorischen Anforderungen. Dabei werden zwei Szenarien gegenübergestellt. Im ersten Szenario wird der Roboter nicht als HRKIS eingestuft, im zweiten hingegen schon. In diesem Fall werden die entsprechend strengeren Anforderungen proaktiv umgesetzt.

«Für ANYbotics ist die Umsetzung verschiedener EU-Regulierungen zentral für den Marktzugang.»
Dr. Christian Gehring, Co-Founder and Sr. Director of Robotics & AI

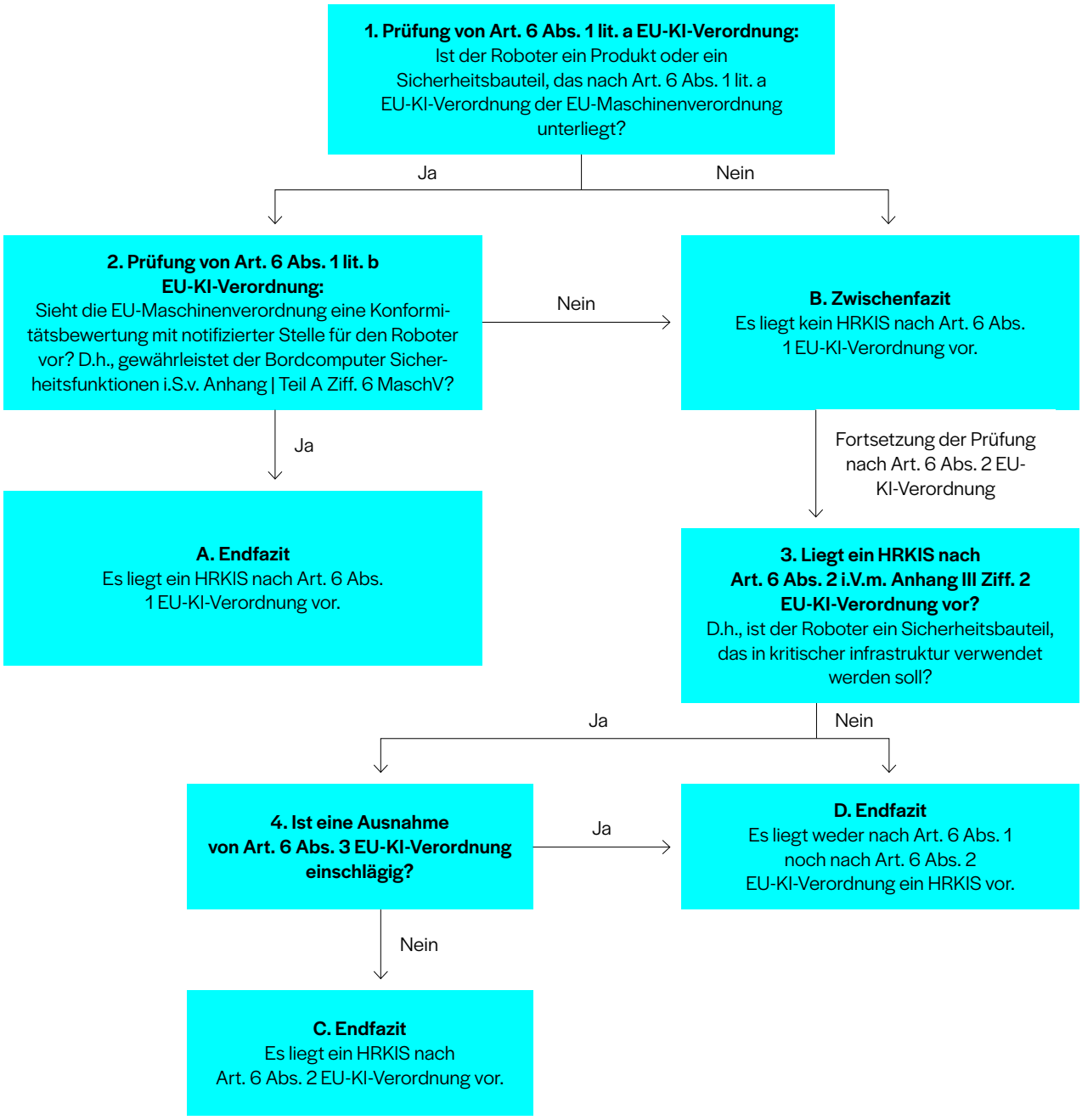
Im ersten Szenario wird argumentiert, dass der Inspektionsroboter nicht als HRKIS einzustufen ist. Der Vorteil dieser Herangehensweise liegt darin, dass Systeme, die nicht als hoch riskant gelten, weniger strenge Anforderungen erfüllen müssen. Der Nachteil ist, dass die Argumente gegen eine Einordnung als HRKIS im konkreten Fall teilweise nicht sehr belastbar sind. Sollte es zu einer behördlichen oder gerichtlichen Beurteilung kommen, besteht das Risiko, dass diese zu einer abweichenden Einschätzung gelangt. Dann müsste der Roboter nach dem neu eingeführten Konformitätsbewertungsverfahren der EU-KI-Verordnung zertifiziert werden. Dieses Verfahren ist bei den zuständigen Prüfstellen (den sog. notifizierten Stellen) noch nicht etabliert, was aus Sicht des Sandbox-Teams zu Unklarheiten, grösserem Aufwand und höheren Zertifizierungskosten führen kann.

Im zweiten Szenario wird argumentiert, dass es sich beim Roboter um ein HRKIS handelt. Der Hersteller setzt in diesem Fall die entsprechenden Anforderungen der EU-KI-Verordnung um. Der Vorteil dieser Strategie besteht darin, dass der Roboter nicht über das neue Konformitätsbewertungsverfahren der EU-KI-Verordnung, sondern über das bereits etablierte Konformitätsbewertungsverfahren der EU-Maschinenverordnung zertifiziert werden kann. Dieses Verfahren ist bei den notifizierten Stellen bereits etablierter – mit Ausnahme der Anforderungen nach EU-KI-Verordnung –, was zu weniger Unsicherheiten und zu geringeren Kosten führt. Nachteilig ist jedoch, dass HRKIS strengere Anforderungen erfüllen müssen als nicht hoch riskante Systeme.

03. Sandbox-Projekt mit ANYbotics

I. Szenario 1: keine Qualifikation als HRKIS

Das Szenario 1 umfasst verschiedene Optionen, mit denen eine Einstufung des Roboters als HRKIS vermieden werden kann. Sie sind in einem Entscheidungsbaum dargestellt, der schrittweise durch die relevanten Prüfungen führt. Ausgangspunkt ist die Analyse der Anforderungen gemäss Artikel 6 Absatz 1 der EU-KI-Verordnung, gefolgt von der Prüfung nach Artikel 6 Absatz 2. Im Anschluss daran werden jene Entscheidungswege erläutert, die aus Sicht des Sandbox-Teams eine vertretbare Grundlage dafür bieten, den Roboter nicht als HRKIS einzuordnen.



03. Sandbox-Projekt mit ANYbotics

Option 1: kein Sicherheitsbauteil
Ein vertretbarer Weg innerhalb des ersten Szenarios ergibt sich aus folgendem Pfad im Entscheidungsbaum:
1. Ja | 2. Nein | 3. Nein → D

Zuerst muss geprüft werden, ob der Roboter ein Produkt oder ein Sicherheitsbauteil nach Artikel 6 Absatz 1 Buchstabe a der EU-KI-Verordnung ist und unter die EU-Maschinenverordnung fällt. Das Sandbox-Team nimmt an, dass dies zutrifft, denn ANYbotics hat den Roboter bislang bereits unter der bisherigen EU-Maschinenrichtlinie bewertet. Diese Annahme wurde allerdings nicht vertieft überprüft. Zu beachten ist, dass die Voraussetzungen der Buchstaben a und b von Artikel 6 Absatz 1 der EU-KI-Verordnung kumulativ erfüllt sein müssen. Wenn also der Roboter kein Sicherheitsbauteil oder Produkt nach Buchstabe a ist, dann muss nicht mehr geprüft werden, ob er nach Buchstabe b einer Konformitätsbewertung unterzogen werden muss. Da es jedoch sehr wahrscheinlich ist, dass Buchstabe a bei ANYmal erfüllt ist, muss geprüft werden, ob auch Buchstabe b erfüllt ist.

Das Sandbox-Team argumentiert, dass der Roboter keiner Konformitätsbewertung nach EU-Maschinenverordnung unterliegt und somit Artikel 6 Absatz 1 Buchstabe b der EU-KI-Verordnung nicht erfüllt ist. Nach Artikel 25 Absatz 2 der EU-Maschinenverordnung unterliegen diejenigen Produkte einer Konformitätsbewertung, die in Anhang I Teil A aufgelistet sind. In diesem Anhang kommt besonders Ziffer 6 für den Roboter infrage. Ziffer 6 setzt jedoch voraus, dass der Roboter über ein «eingebettetes System» verfügt, das Sicherheitsfunktionen gewährleistet. Eine Sicherheitsfunktion ist nach Artikel 3 Ziffer 4 der EU-Maschinenverordnung eine Funktion, die als Schutzmassnahme zur Beseitigung oder Reduzierung eines Risikos dient und deren Ausfall zu einer Erhöhung des Risikos führt. Das im Roboter verbaute eingebettete System, der Bordcomputer, gewährleistet jedoch keine Sicherheitsfunktionen nach dieser Definition. Dies wird damit begründet, dass eine Überprüfung der Sicherheit einer Machine-Learning-Methode – wie sie etwa für das System zur Hindernisvermeidung (Obstacle Avoidance) eingesetzt wird – aus technischen Gründen derzeit nicht möglich ist. Wenn also nicht klar ist, wie sicher das System zur Hindernisvermeidung ist, gewährleistet dieses auch keine Sicherheitsfunktion. Dasselbe gilt für die Module Locomotion und die Inspection Intelligence. Da die Voraussetzungen aus den Buchstaben a und b kumulativ erfüllt sein müssen, führt die Antwort Nein an dieser Stelle zur Schlussfolgerung, dass kein HRKIS gemäss Artikel 6 Absatz 1 EU-KI-Verordnung vorliegt.

Es könnte jedoch auch ein HRKIS nach Artikel 6 Absatz 2 und Anhang III Ziffer 2 EU-KI-Verordnung vorliegen. Hierzu ist erforderlich, dass der Roboter ein Sicherheitsbauteil einer kritischen Infrastruktur ist. Das Sandbox-Team argumentiert, dass der Roboter mangels fester Verbindung zu einer kritischen Infrastruktur nicht als Bauteil gilt. Darüber hinaus übernimmt er – wie bereits ausgeführt – keine Sicherheitsfunktionen. Auf diese Weise entsteht das Ergebnis, dass der Roboter weder gemäss Artikel 6 Absatz 1 noch gemäss Artikel 6 Absatz 2 EU-KI-Verordnung als HRKIS einzustufen ist.

Option 2: Ausnahme gemäss Artikel 6 Absatz 3 EU-KI-Verordnung
Ein alternativer Entscheidungsweg ergibt sich über folgenden Pfad:
1. Ja | 2. Nein | 3. Ja | 4. Ja → D

Hier nimmt das Sandbox-Team mit derselben Argumentation wie bei Option 1 an, dass kein HRKIS nach Artikel 6 Absatz 1 EU-KI-Verordnung vorliegt. Hingegen geht es davon aus, dass der Roboter ein Sicherheitsbauteil einer kritischen Infrastruktur dar-

stellt. Die Argumentation lautet, dass bei Ausfall des Roboters ein erhöhtes Risiko für die Sicherheit oder Gesundheit von Menschen entstehen kann und damit ein Sicherheitsbauteil im Sinne von Artikel 3 Ziffer 14 EU-KI-Verordnung vorliegt. Zusätzlich wird vertreten, dass der Begriff «Sicherheitsbauteil» nicht nur im wörtlichen Sinne auszulegen ist, sodass auch ein nicht fest verbautes System wie der Roboter als Bauteil gelten kann. Demnach liegt ein HRKIS nach Artikel 6 Absatz 2 EU-KI-Verordnung vor.
Schliesslich sind die Ausnahmen nach Artikel 6 Absatz 3 EU-KI-Verordnung zu prüfen. Trifft eine dieser Ausnahmen zu, dann liegt trotz der Erfüllung der Voraussetzungen von Artikel 6 Absatz 2 EU-KI-Verordnung kein HRKIS vor. Hier wird argumentiert, dass der Roboter keine eigenständigen Entscheidungen trifft, sondern lediglich vorbereitende Tätigkeiten für menschliche Entscheidungsträgerinnen und -träger übernimmt. Damit ist die Ausnahme gemäss Artikel 6 Absatz 3 Buchstabe d EU-KI-Verordnung einschlägig, und es liegt kein HRKIS vor. Insgesamt führt auch dieser Pfad zum Ergebnis, dass der Roboter weder nach Artikel 6 Absatz 1 noch nach Artikel 6 Absatz 2 EU-KI-Verordnung als HRKIS einzustufen ist.

Option 3: Nutzung von Übergangsvorschriften
Eine dritte Möglichkeit innerhalb des ersten Szenarios besteht darin, sich auf die Übergangsbestimmungen der EU-KI-Verordnung zu berufen. Nach Artikel 111 gilt die EU-KI-Verordnung für bereits auf dem Markt befindliche KI-Systeme nicht, sofern diese vor dem 2. August 2026 in Verkehr gebracht oder in Betrieb genommen wurden – es sei denn, es erfolgt eine wesentliche Veränderung der Konstruktion. Unklar bleibt jedoch, was unter einer wesentlichen Veränderung zu verstehen ist. Die EU-KI-Verordnung definiert eine «wesentliche Veränderung» als eine Änderung, die in der ursprünglichen, vom Anbieter durchgeführten Konformitätsbewertung nicht vorgesehen oder geplant war und entweder die Konformität des KI-Systems beeinträchtigt oder zu einer Änderung der Zweckbestimmung führt, für die das System bewertet wurde. Eine wesentliche Veränderung liegt somit nur dann vor, wenn infolge der Änderung die Einhaltung der EU-KI-Verordnung nicht mehr gewährleistet ist. In Anlehnung an die bisherige Praxis zur EU-Maschinenrichtlinie kann dabei darauf abgestellt werden, ob durch die Änderung eine neue Gefährdung entsteht oder ein bestehendes Risiko für die von der EU-KI-Verordnung geschützten Rechtsgüter erhöht wird.

«EU-Regulierungen wirken oft weniger drastisch auf Firmen als erwartet – wer Spielräume klug nutzt und Risiken pragmatisch analysiert, kann eine passende Strategie entwickeln.» *Sven Kohlmeier, Fachanwalt für IT-Recht (DE), Wicki Partners AG*

Fazit zum ersten Szenario
Dieses Szenario bietet die Möglichkeit, die Einstufung des Roboters als HRKIS zu vermeiden. Ob die entsprechende Argumentation jedoch einer gerichtlichen Überprüfung standhalten würde, ist derzeit offen, da Rechtsprechung zu diesen Fragestellungen bislang fehlt. Vor dem Hintergrund des geopolitischen Wettbewerbs, etwa mit Blick auf die technologische Konkurrenz durch die USA, könnte eine weite Auslegung der EU-KI-Verordnung durch die EU gefördert werden. Wird der Roboter nicht als HRKIS eingestuft, unterliegt er keinen Konformitätsbewertungsverfahren nach EU-KI-Verordnung und muss lediglich die grundlegenden Anforderungen der Verordnung an KI-Systeme erfüllen. Allerdings könnte ein Konformitätsverfahren nach EU-Maschinenverordnung erforderlich bleiben. Ergänzend oder alternativ zur Argumentation gegen eine Qualifikation als HRKIS (Optionen 1 und 2) kann die Übergangsregelung (Option 3) genutzt werden, um die Anwendung der EU-KI-Verordnung vorläufig zu vermeiden.

II. Szenario 2: Qualifikation als HRKIS
In diesem Szenario wird angenommen, dass der Roboter künftig der neuen EU-Maschinenverordnung unterliegt und gemäss dieser durch eine notifizierte Stelle zertifiziert werden muss. Da damit die Voraussetzungen von Artikel 6 Absatz 1 Buchstabe a und b erfüllt sind, liegt ein HRKIS vor.

Zertifizierung nach EU-Maschinenverordnung
Wenn ein HRKIS vorliegt, empfiehlt das Sandbox-Team den Herstellern, zunächst das Konformitätsbewertungsverfahren nach EU-Maschinenverordnung durchzuführen. Dabei prüft die notifizierte Stelle gleichzeitig die Einhaltung der Anforderungen der EU-KI-Verordnung. Eine Zertifizierung nach EU-KI-Verordnung ist daher nicht erforderlich. Auf diese Weise müssen die Hersteller also ausschliesslich das bereits etablierte Verfahren durchlaufen. Das potenziell teurere, neue Verfahren nach EU-KI-Verordnung kann vermieden werden.
Entscheidend ist, dass nach EU-Maschinenverordnung nicht der gesamte Roboter zertifiziert werden muss, sondern nur der sogenannte Bordcomputer – also die Steuerungseinheit, in der die KI-Funktionen verankert sind. Zertifizierungspflichtig sind «eingebettete Systeme mit selbstentwickelndem Verhalten», deren Ausfall das Risiko für Personen erhöht. Entsprechend könnten laut Diskussion mit dem Hersteller insbesondere folgende Module des Roboters zertifizierungspflichtig sein:

- **Obstacle Avoidance**
  Ein Ausfall könnte zu Unfällen führen.
- **Inspection Intelligence**
  Ein Defekt könnte Risiken (z.B. unbeachtete Lecks) verursachen.
- **Locomotion**
  Ein Fehler könnte dazu führen, dass der Roboter stürzt und damit eine Gefährdung verursacht.

03. Sandbox-Projekt mit ANYbotics

Für die Zertifizierung des Bordcomputers stehen drei Verfahren zur Auswahl (siehe dazu Kapitel 2.1):

1. **EU-Baumusterprüfung**
   am besten geeignet; ein einzelnes Modell wird geprüft, keine laufenden Audits
2. **Umfassende Qualitätssicherung**
   ungeeignet wegen unangekündigter Audits
3. **Einzelprüfung**
   ungeeignet für Serienprodukte wegen hoher Kosten

Die übrigen Komponenten des Roboters, wie Beine oder Gehäuse, können weiterhin mit der internen Fertigungskontrolle geprüft werden.

Fazit zum zweiten Szenario
Die Argumentation im zweiten Szenario erfordert nur eine einzige Zertifizierung durch eine notifizierte Stelle – nämlich nach EU-Maschinenverordnung. Dabei wird gleichzeitig die Konformität mit der EU-KI-Verordnung geprüft. Nur der Bordcomputer muss extern zertifiziert werden, während der Rest des Roboters intern geprüft werden kann. Das geeignetste Konformitätsbewertungsverfahren für ANYbotics ist die EU-Baumusterprüfung. Weiter müssen die Pflichten für HRKIS-Anbieter gemäss EU-KI-Verordnung beachtet werden. Die Vorteile des zweiten Szenarios liegen in einem geringeren rechtlichen Risiko und in etablierten Verfahren. Nachteilig ist, dass höhere Anforderungen zu erfüllen sind als beim ersten Szenario.

Handlungsempfehlungen

Die Entscheidung zwischen den unterschiedlichen Argumentationsszenarien ist nicht allein juristisch zu treffen, sondern setzt auch eine unternehmerische Abwägung voraus. Sollte der Roboter ohnehin unter die EU-Maschinenverordnung fallen, empfiehlt das Sandbox-Team, die Umsetzungsstrategie aus Szenario 2 zu wählen, das Zertifizierungsverfahren nach EU-Maschinenverordnung zu durchlaufen – idealerweise in Form der EU-Baumusterprüfung – und damit gleichzeitig die Anforderungen der EU-KI-Verordnung abzudecken.

03. Sandbox-Projekt mit ANYbotics

Checkliste für Hochrisikosysteme

Für die Anbieter von HRKIS stellt die EU-KI-Verordnung einige Pflichten auf. Die EU-Maschinenverordnung enthält Pflichten für Hersteller von Maschinen, die deckungsgleich oder ähnlich sind (siehe vierte Spalte). Daher sind mit dem Durchlaufen des Konformitätsbewertungsverfahrens nach der EU-Maschinenverordnung schon einige Pflichten nach der EU-KI-Verordnung zumindest teilweise erfüllt. Hier sind alle Pflichten als Checkliste aufgelistet, die die EU-KI-Verordnung Anbietern von HRKIS auferlegt:

Erledigt	Pflicht	Artikel in der EU-KI-Verordnung	Ähnliche Pflicht nach EU-Maschinenverordnung
◌	Anbringen von Name, Marke und Kontaktanschrift	16 b)	10 VI
◌	Einrichten eines Qualitätsmanagementsystems	16 c), 17	Bei umfassender Qualitätssicherung: Anhang IX Ziffer 3; bei Einzelprüfung: Anhang X Ziffer 2 Unterabsatz 3 ii)
◌	Erstellen und Aufbewahren von Dokumentationen	16 d), 11, 17, 47, 18	10 II, Anhang IV Teil A
◌	Aufbewahren von automatisch erstellten Protokollen (Logs) für 6 Monate	16 e), 12, 19	Anhang III Teil B Ziffer 1.2.1. Unterabsatz 3 b): Aufbewahren für 1 Jahr
◌	Durchführen eines Konformitätsbewertungsverfahrens (im Fall ANYbotics nach EU-Maschinenverordnung)	16 f), 43 III, Verordnung (EU) 2023/1230	10 II, 25
◌	Ausstellen einer EU-Konformitätserklärung	16 g), 47	10 II
◌	Anbringen einer CE-Kennzeichnung	16 h), 48	10 II
◌	Ergreifen von Korrekturmassnahmen, falls HRKIS nach Inverkehrbringen nicht (mehr) mit der EU-KI-Verordnung konform	16 j)	10 IX
◌	Bei Nachfrage durch Behörde: Nachweis der Erfüllung der Anforderungen an HRKIS	16 k), 8–15	10 X
◌	Einrichten eines Risikomanagementsystems	9	Anhang IV Teil A b): Risikobeurteilung
◌	Erstellen einer technischen Dokumentation, die Angaben nach EU-KI- und EU-Maschinenverordnung enthält	11, Anhang IV, Verordnung (EU) 2023/1230	Anhang IV Teil A
◌	Erstellen einer Betriebsanleitung, die transparente Bedienung ermöglicht	13	10 VII
◌	Beaufsichtigung durch Menschen	14	Anhang III Teil B Ziffer 3.2.4
◌	Gewährleisten von genügender Genauigkeit, Robustheit und Cybersicherheit	15	Anhang III Teil B Ziffer 1.1.9: Schutz vor Korrumpierung
◌	Barrierefreier Zugang zu Websites und Produkten	16 l), Richtlinie (EU) 2016/2102, Richtlinie (EU) 2019/882	
◌	Einrichten eines Data-Governance-Verfahrens, damit die Trainingsdaten möglichst fehler- und biasfrei sind	10	
◌	Einrichten eines Systems zur Beobachtung des HRKIS nach Inverkehrbringen (Kunden von ANYbotics müssen hierzu Daten weiterleiten)	72	
◌	Melden schwerwiegender Vorfälle an Marktüberwachungsbehörde	73	
◌	Wenn Behörde dies vorsieht: Prüfung der Konformität mit EU-KI-Verordnung durch Marktüberwachungsbehörde	79, Verordnung (EU) 2019/1020	
Entfällt	Registrierung in der EU-Datenbank für HRKIS nach Anhang III (ANYbotics fällt nicht unter Anhang III)	16 i), 49, 71, Anhang III	

3.3. KI-Governance und ISO/IEC 42001

Unabhängig davon, ob ein autonomer Inspektionsroboter regulatorisch als HRKIS qualifiziert wird oder nicht, gewinnt eine systematische KI-Governance zunehmend an Bedeutung. Denn die regulatorischen Anforderungen in den Bereichen KI, Cybersicherheit, Produktsicherheit und Datenzugang werden in den kommenden Jahren weiter zunehmen – sowohl in der EU als auch weltweit.

Eine strukturierte Governance ermöglicht es, bestehende und künftige Anforderungen gezielt zu berücksichtigen, ohne für jedes neue Regulierungsinstrument ein separates Konzept entwickeln zu müssen. Denn in einem zentral verankerten KI-Management-System lassen sich verschiedene regulatorische Vorgaben abbilden – etwa solche aus der EU-KI-Verordnung, aber auch KI-bezogene Vorgaben aus der EU-Maschinenverordnung oder KI-Regulierungen in anderen Regionen, die als Markt interessant sind.

Im folgenden Abschnitt wird anhand von *ISO/IEC 42001*[3] ein möglicher Umsetzungsansatz für eine solche KI-Governance vorgestellt. Die internationale Norm definiert erstmals ein strukturiertes Managementsystem speziell für den verantwortungsvollen Einsatz von KI. Sie baut auf etablierten Prinzipien des Informationssicherheits- und Qualitätsmanagements auf und überträgt diese auf KI-spezifische Risiken und Steuerungsprozesse. Das Konzept eines KI-Management-Systems wurde im Rahmen des Sandbox-Projekts mit ANYbotics in Zusammenarbeit mit dem Zürcher Unternehmen Modulos AG praktisch getestet. Ziel war es, ein schlankes, System vorzubereiten, das regulatorische Anforderungen strukturiert adressiert und gleichzeitig als modulare Grundlage dient, um bei Bedarf gezielt regulatorische Lücken (z.B. aus der EU-KI-Verordnung oder der EU-Maschinenverordnung) zu füllen.

Dabei sind die Erfahrungen aus dem Anwendungsfall eingeflossen – insbesondere bei der Systemabgrenzung, bei der organisatorischen Verankerung sowie bei ausgewählten Dokumentations- und Steuerungsinstrumenten.

«Wer KI-Governance systematisch verankert, schafft Sicherheit, reduziert Risiken und gewinnt langfristig Marktzugang.» *Elena Maran, Global Head of Responsible AI, Modulos AG*

Motivation und Zielsetzung

Das Ziel war, die Einführung eines KI-Management-Systems gemäss den Anforderungen der ISO/IEC 42001 vorzubereiten – als ersten konkreten Schritt zur Verankerung einer KI-Governance im Unternehmen. Dies erfolgte vor dem Hintergrund, dass zum Zusammenspiel zwischen der EU-KI-Verordnung und der EU-Maschinenverordnung noch keine abschliessende Rechtsklarheit besteht. Die Entscheidung, ein KI-Management-System einzuführen, wurde durch mehrere zusammenwirkende Faktoren motiviert. Zum einen ist ANYbotics in stark regulierten Branchen tätig – darunter Öl und Gas, Bergbau, chemische Industrie und Energieerzeugung – und agiert in über 20 Ländern. Zum anderen bilden KI-Technologien einen wesentlichen Bestandteil des Produkts des Unternehmens, und die Einhaltung regulatorischer Anforderungen gewinnt zunehmend an Bedeutung – insbesondere im Hinblick auf die

[3] Vgl. ISO/IEC 42001:2023 «Information technology – Artificial intelligence – Management system» (abrufbar als textgleiche Schweizer Norm SN ISO/IEC 42001:2025 unter: https://connect.snv.ch/de/sn-isoiec-42001-2025). Herstellern wird empfohlen, die Norm frühzeitig als Orientierungsrahmen für den Aufbau eines KI-Management-Systems zu nutzen und sie mit bestehenden Qualitäts- und Sicherheitsstandards zu verzahnen.

03. Sandbox-Projekt mit ANYbotics

potenzielle Einstufung autonomer Robotersysteme als Hochrisikoanwendungen gemäss EU-KI-Verordnung. Zusätzlich haben Kundenanforderungen an die KI-Governance und der Wunsch nach wettbewerblicher sowie verantwortungsvoller KI-Entwicklung das Vorhaben, ein umfangreiches KI-Governance-Framework anzustreben, begünstigt. Zudem erhöht ein implementiertes KI-Management-System das Vertrauen der Kunden.

Technische Herausforderungen und regulatorische Komplexität
Im Rahmen der Vorbereitung des KI-Management-Systems bei ANYbotics traten typische Herausforderungen auf, wie sie bei KI-gestützten Robotiksystemen im industriellen Umfeld regelmässig zu beobachten sind. Besonders relevant sind die folgenden Punkte:

- **Autonome Navigation in sicherheitskritischen Umgebungen**
  Der Einsatz von ANYmal in Anlagen wie Raffinerien, Chemieanlagen oder Kraftwerken bringt erhebliche Sicherheitsanforderungen mit sich. Eine fehlerhafte Navigation oder Fehlentscheidungen der KI können in solchen Kontexten schwerwiegende Folgen haben.
- **Integration von Drittanbieter-KI-Komponenten**
  Für zentrale Funktionen wie die Bildverarbeitung werden teilweise externe KI-Module eingesetzt. Die Validierung, die Nachvollziehbarkeit und die langfristige Wartung solcher Komponenten sind besonders anspruchsvoll – insbesondere im Hinblick auf regulatorische Anforderungen.
- **Modell-Drift unter realen Einsatzbedingungen**
  Unterschiedliche Lichtverhältnisse, strukturelle Veränderungen in Anlagen, Witterungseinflüsse oder Verschmutzungen können die Leistung von KI-Modellen im Feld verändern. Die Stabilität und die Robustheit der Modelle müssen daher laufend überwacht und getestet werden.
- **Regulatorische Vielfalt in über 20 Einsatzländern**
  ANYbotics ist international tätig und muss regulatorische Vorgaben aus verschiedenen Jurisdiktionen erfüllen. Die Abstimmung zwischen der EU-KI-Verordnung, der EU-Maschinenverordnung und weiteren nationalen Regelwerken stellt eine erhebliche Herausforderung dar.
- **Hohe Updatefrequenz und Versionskontrolle**
  Das System wird in vierteljährlichen Zyklen weiterentwickelt. Dies erfordert stringente Prozesse zur Versionierung, Testdokumentation, Freigabe und Rückverfolgbarkeit – insbesondere bei sicherheitskritischen Komponenten.

Das Robotersystem ANYmal kombiniert fortschrittliche KI wie Deep Learning oder Reinforcement Learning und generative KI für Computer Vision, Navigation und Inspektion. Gerade diese technische Komplexität unterstreicht die Notwendigkeit eines strukturierten, risikobasierten KI-Governance-Ansatzes – sowohl um regulatorische Anforderungen zu erfüllen als auch um Sicherheit, Qualität und Skalierbarkeit im Betrieb sicherzustellen. Die bestehenden Information-Security-Management- und Safety-Strukturen waren eine wichtige Grundlage, um KI-spezifische Risiken mit eigenständigen, spezialisierten Governance-Strukturen zu adressieren.

Risikobewertung
Die Risikoanalyse ergab für ANYbotics ein mittleres Risiko, das durch das komplexe regulatorische Umfeld, den autonomen Einsatz der Systeme sowie die technologische Komplexität der KI-Komponenten geprägt ist. Zwar reduzieren das bestehende Information-Security-Management-System und etablierte Risikomanagementprozesse die Verwundbarkeit, jedoch besteht insbesondere beim Aufbau dedizierter Ressourcen für KI-Governance noch Entwicklungspotenzial.

03. Sandbox-Projekt mit ANYbotics

Bewertung Gesamtrisiko Mittel		
Extern **Regulatorischen Kontext bewerten** ▪ EU-KI-Verordnung (potenzielle Einstufung als Hochrisikosystem) ▪ Einhaltung mehrerer Jurisdiktionen ▪ Dynamische/ fortlaufende Weiterentwicklung des Regulierungsumfelds	**Operativ** **Betrieblichen Einsatz beurteilen** ▪ Sicherstellung menschlicher Aufsicht im Betrieb ▪ Echtzeitengscheidungsfindungen ▪ Sicherheitskritische Umgebungen	**Technisch** **Systemautonomie einschätzen** ▪ Herausforderungen bei Zuverlässigkeit und Robustheit ▪ Intransparenz von Reinforcement-Learning-Systemen ▪ Modell-Drift und Datenqualität

Zentrale KI-Risiken
Die umfassende Risikoanalyse hat zehn kritische Risiken identifiziert, die sich auf drei miteinander verbundene Kategorien verteilen.

1. **Externe Risiken** konzentrieren sich auf das komplexe regulatorische Umfeld sowie auf Herausforderungen im Stakeholder-Management. Schwierigkeiten bei der regulatorischen Konformität resultieren aus sich ständig weiterentwickelnden KI-Vorgaben in unterschiedlichen Rechtsräumen. Gleichzeitig zeigen sich Risiken gegenüber Stakeholdern, insbesondere bei der klaren Vermittlung der Fähigkeiten und Grenzen der KI-Systeme gegenüber Industriepartnern, die oft in risikoaversen Umfeldern operieren.
2. **Operationelle Risiken** entstehen durch die besonderen Anforderungen beim Einsatz autonomer Systeme mit Echtzeitentscheidungsfindung in sicherheitskritischen Kontexten. Um potenzielle Sicherheitsrisiken zu vermeiden, ist es essenziell, dass die Systeme von Menschen überwacht werden können. Lücken in der übergeordneten KI-Governance machen zudem deutlich, dass strukturierte Verantwortlichkeitsmechanismen erforderlich sind. Herausforderungen im Updatemanagement ergeben sich aus dem vierteljährlichen Roll-out-Zyklus, während Risiken der Laufzeitkompromittierung die Anfälligkeit autonomer Systeme für gezielte Angriffe unterstreichen – mit potenziellen Auswirkungen auf Betriebssicherheit und Funktionsfähigkeit.
3. **Technische Risiken** dominieren die Bewertung. Sie umfassen grundlegende Herausforderungen in Bezug auf die Zuverlässigkeit und die Robustheit von KI-Systemen in unvorhersehbaren industriellen Umgebungen sowie die inhärente Intransparenz von Entscheidungsprozessen in komplexen Reinforcement-Learning-Systemen. Besonders hervorzuheben ist das Risiko des Modell-Drift, das auf die dynamischen Bedingungen in Inspektionsumgebungen zurückzuführen ist. Hinzu kommen Herausforderungen bei der Datenqualität sowie KI-spezifische Sicherheitslücken, die fortlaufende operationelle Hürden darstellen und gezielte Gegenmassnahmen erfordern.

03. Sandbox-Projekt mit ANYbotics

Category	Risk	Impact	Controls
Technical	AI System Reliability and Robustness	Critical	A. 6.2.4, A.6.2.6
Technical	Opacity of Decision-Making	High	A. 6.2.3, A.6.2.7
Technical	AI Model Drift	Medium	A. 6.2.6, A. 6.2.8
Technical	Data Quality Issues	High	A.7.4, A.7.6
Technical	AI-Specific Security Vulnerabilities	High	A. 6.2.3, A.6.2.7
Operational	AI Update Management	Medium	A. 6.2.5, A.6.2.6
Operational	AI Governance Gaps	Critical	A. 2.2, A.3.2
Operational	Runtime AI System Compromise	High	A. 6.2.5, A. 6.2.6, A.9.4
Technical	Regulatory Compliance	High	A.2.3, A.8.5
Technical	Stakeholder Communication	Medium	A.8.2, A.8.4

Erklärung zur Anwendbarkeit

Die zehn identifizierten Risiken bildeten die Grundlage für die Auswahl und die Priorisierung der im KI-Management-System umgesetzten Kontrollmassnahmen. Dabei zeigte sich, dass viele der Herausforderungen im technischen und im operationellen Bereich spezifische Governance-Instrumente erfordern. Basierend auf der Doppelrolle von ANYbotics als KI-Anbieter und -Hersteller mit einem mittleren Risiko umfasst das Statement of Applicability alle wesentlichen Kontrollen aus Anhang A der ISO/IEC 42001, mit Ausnahme der Bewertung gesellschaftlicher Auswirkungen (A.5.5). Diese wurde aufgrund des begrenzten Anwendungskontexts im Bereich industrieller Inspektionen ausgeschlossen. Im Fokus der relevanten Kontrollen stehen insbesondere:

- **KI-Richtlinien (A.2)**
- **Governance-Rollen (A.3)**
- **Lebenszyklusmanagement (A.6)**
- **Daten-Governance (A.7)**
- **Verantwortungsvoller Einsatz (A.9)**

Risikobasierte Priorisierung der Implementierungskontrollen

Die Priorisierung der Kontrollen basierte auf einem mittleren Risiko, der Doppelrolle als KI-Anbieter und -Hersteller, der vorhandenen Information-Security-Management-Struktur sowie auf dem Umstand, dass keine sensitiven Personendaten verarbeitet werden. Dadurch konnte gezielt auf jene Anforderungen fokussiert werden, die für die industrielle

03. Sandbox-Projekt mit ANYbotics

Robotik besonders relevant sind – etwa Systemzuverlässigkeit, strukturelle Governance und KI-spezifische Sicherheitsaspekte. Die Umsetzungs-Roadmap priorisierte drei kritische Risiken:

1. **Zuverlässigkeit und Robustheit der KI-Systeme**
   Aufbau von Verifizierungs- und Validierungsprozessen sowie von umfassenden Monitoring-Frameworks (bspw. durch Machine Learning Operations)
2. **Lücken in der KI-Governance**
   Etablierung formeller Governance-Strukturen und Definition von Rollen und Zuständigkeiten
3. **KI-spezifische Sicherheitslücken**
   Dokumentation von Sicherheitskontrollen und Umsetzung gezielter Strategien zur Schwachstellenminimierung

Dieser strukturierte und risikoorientierte Ansatz ermöglichte eine zielgerichtete Einführung des KI-Management-Systems bei gleichzeitig effizientem Ressourceneinsatz – ohne flächendeckende Überforderung der Organisation.

Priority	Risk	Controls	Control Descriptions
◌	AI System Reliability and Robustness	A.6.2.4, A.6.2.6	Verification and validation processes, monitoring framework
◌	AI Governance Gaps	A.2.2, A.3.2	Establish governance structure, define roles and responsibilities
◌	AI-Specific Security Vulnerabilities	A.6.2.3, A.6.2.7	Document security controls, vulnerability mitigation

Empfehlungen für ähnliche Organisationen
Die Erfahrung von ANYbotics zeigt mehrere kritische Erfolgsfaktoren für die Implementierung der ISO/IEC 42001:

- **Managementsupport** ist entscheidend. Die Unterstützung durch das Management ist essenziell für die Ressourcenbereitstellung und das Überwinden interner Hürden während der Governance-Transformation.
- **Auf bestehenden Strukturen aufbauen** statt bei null anfangen. Die etablierten Information-Security-Management- und Safety-Prozesse bilden ein solides Fundament. Das zeigt, wie bestehende Governance-Strukturen genutzt und erweitert werden können – mit Zeitgewinn und minimaler Störung operativer Abläufe.
- **Externe Expertise** ist ein zentraler Erfolgsfaktor. Die Unterstützung durch spezialisierte Beraten-

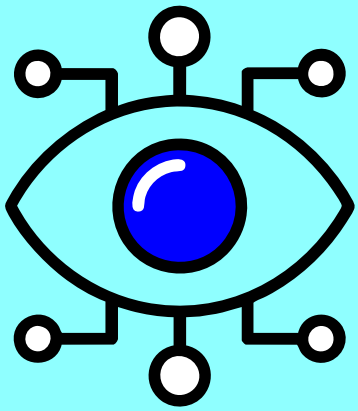
de bei der Gap-Analyse ermöglicht es, typische Fallstricke zu vermeiden und das organisationsinterne Lernen zu beschleunigen – besonders in Bereichen mit geringer interner Governance-Erfahrung.

- **Eine umfassende Risikoanalyse** ist die Grundlage für alle weiteren Schritte. Nur so lassen sich Ressourcen auf die wirkungsvollsten Massnahmen fokussieren.
- **Eine lückenlose Dokumentation** aller Prozesse und Entscheidungen schafft die für eine Zertifizierung notwendige Nachvollziehbarkeit.
- **Quick Wins** im Projektverlauf helfen zudem, die Motivation über den langen Implementierungszeitraum hinweg aufrechtzuerhalten.

Herausforderungen für die Umsetzung
Organisationen sollten auch typische Fehler vermeiden:

- Eine **gleichzeitige Umsetzung in allen Bereichen** überfordert die Teams und lenkt von prioritären Risiken ab.
- Das **Auslassen von Impact-Assessments** führt zu blinden Flecken, die spätestens bei der Auditierung aufgedeckt werden.
- Die **Isolation von bestehenden Governance-Strukturen** verursacht unnötige Zielkonflikte und Doppelspurigkeit.
- Häufig wird der **kulturelle Wandel** unterschätzt – fehlendes Change-Management verlangsamt die Akzeptanz.
- Ein verspäteter Aufbau von **Monitoring-Systemen** verhindert die frühzeitige Erkennung von Umsetzungslücken, was später zu deutlich höheren Kosten führen kann.

04.
Fazit und Ausblick



Auf Basis der rechtlichen Analyse der wichtigsten EU-Regulierungen sowie der praktischen Erfahrungen aus dem Anwendungsfall ergeben sich zentrale Handlungsfelder für Unternehmen. Die folgenden Abschnitte bündeln diese Erkenntnisse in Form übergreifender Empfehlungen für Regulierung, Risikomanagement und Innovationsförderung.

---

1. **Systematische Integration regulatorischer Anforderungen**
   Die zunehmende Regulierungsdichte im Bereich KI und Robotik verlangt ein systematisches Vorgehen, um neue Vorgaben konsequent in bestehende Entwicklungs- und Steuerungsprozesse einzubetten. Am Beispiel autonomer Inspektionsroboter zeigt sich, dass Unternehmen technische Innovationen frühzeitig mit regulatorischen Anforderungen rückkoppeln müssen – insbesondere bei sicherheitskritischen Funktionen und beim Einsatz in kritischen Infrastrukturen. Ziel ist es, ein konsistentes Governance-Framework zu etablieren, das neue gesetzliche Vorgaben wie die EU-KI-Verordnung, die EU-Maschinenverordnung oder die EU-Cyberresilienzverordnung ebenso integriert wie freiwillige Standards, etwa die ISO/IEC 42001. So können Unternehmen regulatorische Entwicklungen frühzeitig erkennen, Abhängigkeiten verstehen und bestehende Strukturen effizient weiterentwickeln, ohne für jedes neue Regelwerk separate Systeme aufbauen zu müssen. Erfahrungen aus Testumgebungen wie der KI-Sandbox belegen zudem, dass interdisziplinäre Zusammenarbeit entscheidend dazu beiträgt, Anforderungen praxisnah zu operationalisieren und nachhaltig in der Unternehmenssteuerung zu verankern.

2. **Rolle von Standards und Managementsystemen**
   Freiwillige Normen gewinnen neben gesetzlichen Vorgaben zunehmend an Bedeutung – sowohl für die interne Steuerung als auch für die externe Vertrauensbildung. Mit der ISO/IEC 42001 liegt erstmals eine Norm für ein strukturiertes KI-Management-System vor. Für Unternehmen, die KI in sicherheitskritischen Anwendungsfeldern wie der autonomen Inspektion einsetzen, kann diese Norm mittelfristig einen Wettbewerbsvorteil schaffen, etwa bei Ausschreibungen, internationalen Partnerschaften oder branchenspezifischen Leitlinien. Das Sandbox-Projekt mit ANYbotics und Modulos verdeutlicht, dass die ISO/IEC 42001 insbesondere in Verbindung mit EU-Regulierungen wie der KI-Verordnung – etwa in den Bereichen Risikomanagement und Dokumentationspflichten – wertvolle Orientierung bietet.

04. Fazit und Ausblick

3. **Kombination klassischer und KI-spezifischer Anforderungen**
   Künftige Regulierungsrahmen müssen klassische Sicherheitsanforderungen, wie sie etwa die EU-Maschinenverordnung definiert, konsequent mit den Eigenschaften dynamischer, lernfähiger KI-Systeme verbinden. Ein risikobasierter Ansatz bildet dabei den Kern: Er berücksichtigt physische Gefahren ebenso wie digitale und algorithmische Risiken. Adaptive Konformitätsbewertungen richten sich gezielt auf KI-spezifische Eigenschaften, etwa lernfähige Algorithmen, sich verändernde Modelle oder kontextabhängige Entscheidungslogiken. Abhängig von der Risikostufe sollen differenzierte Prüf- und Nachweisanforderungen gelten – von technischer Dokumentation für statische Systeme über die Validierung von Trainingsdaten und Modellen bei lernenden Systemen bis hin zu externen Audits für sicherheitskritische, nicht deterministische Anwendungen. Ergänzend sichern kontinuierliche Monitoring- und Updatepflichten die Einhaltung von Sicherheits- und Compliance-Anforderungen auch nach dem Inverkehrbringen.

4. **Abgrenzung von KI-Systemen in komplexen Robotikanwendungen**
   Ein zentrales Thema in der Risikobewertung und Regulierung komplexer Robotiksysteme ist die Frage, ob das Gesamtsystem oder einzelne KI-Komponenten betrachtet werden sollen. Während eine Systembewertung die Wechselwirkungen verschiedener Module abdeckt, kann eine komponentenbasierte Bewertung dann sinnvoll sein, wenn einzelne KI-Bausteine – etwa für Navigation oder Bewegungssteuerung – in unterschiedlichen Produkten wiederverwendet werden. Für die Risikoanalyse ist zudem entscheidend, ob die Anwendung (z.B. das Nichterkennen eines Defekts) oder die Betriebssicherheit des Roboters selbst (z.B. eine physische Fehlfunktion) im Vordergrund steht. Ein klar abgegrenztes Bewertungsmodell unterstützt nicht nur die regulatorische Nachvollziehbarkeit, sondern ermöglicht auch eine flexible Wiederverwendung zertifizierter Module in verschiedenen Kontexten. Unternehmen sollten deshalb frühzeitig dokumentieren, auf welcher Ebene die Bewertung erfolgt, und ihre Risikomanagementstrategien entsprechend differenzieren. So lassen sich regulatorische Anforderungen konsistent erfüllen, während gleichzeitig Synergien in der Entwicklung und der Zertifizierung genutzt werden können.

5. **KI-Testumgebungen als Lernräume**
   Testumgebungen für autonome Inspektionsroboter schaffen interdisziplinäre Lernräume, in denen Unternehmen, Forschungseinrichtungen und Behörden gemeinsam Sicherheit, KI-Verhalten und regulatorische Anforderungen in der Praxis erproben können. Regulatorische Experimentierklauseln oder Pilotartikel ermöglichen es, zeitlich und sachlich begrenzt von bestehenden gesetzlichen Vorgaben abzuweichen, um innovative KI-Systeme unter realitätsnahen Bedingungen zu testen. Dabei bleibt die behördliche Aufsicht zentral, ergänzt durch Schutzmassnahmen für Sicherheit und Grundrechte. Solche Testumgebungen leisten damit einen wesentlichen Beitrag dazu, regulatorische Anforderungen praxisnah umzusetzen und Innovation verantwortungsvoll zu fördern.

«Zukunftsfähige Robotik entsteht, wenn technischer Fortschritt und KI-Governance Hand in Hand gehen.»
Raphael von Thiessen, Programmleiter KI-Sandbox, Kanton Zürich

Glossar

ATEX-Zertifizierung
EU-Zertifizierung für Geräte, die in explosionsgefährdeten Bereichen eingesetzt werden. Eine ATEX-Zertifizierung ist die Voraussetzung für den Betrieb autonomer Roboter wie ANYmal X in sensiblen Industrieumgebungen.

Digitale Zwillinge
Virtuelle Abbilder physischer Systeme, die kontinuierlich mit Echtzeitdaten gespeist werden. Sie dienen der Zustandsüberwachung, der Simulation und der Entscheidungsunterstützung – insbesondere bei autonomer Inspektion und vorausschauender Wartung.

EU-Cyberresilienzverordnung (Cyber Resilience Act)
EU-Verordnung zur Verbesserung der Cybersicherheit vernetzter digitaler Produkte und Dienste. Sie legt Anforderungen an Design, Entwicklung und Wartung fest – mit direkter Relevanz für KI-basierte, netzwerkfähige Robotiksysteme.

EU-Datenverordnung (Data Act)
EU-Verordnung zur Förderung der fairen Nutzung und Weitergabe von Daten. Sie regelt insbesondere den Zugang zu und die Nutzung von Daten, die durch vernetzte Geräte oder Dienste erzeugt werden – mit Auswirkungen auf KI-gestützte Inspektionssysteme.

EU-KI-Verordnung (AI Act)
EU-Verordnung zur Regulierung von künstlicher Intelligenz. Sie klassifiziert KI-Systeme in Risikostufen (z.B. gering, hoch oder unzulässig) und legt spezifische Anforderungen an Entwicklung, Transparenz, Sicherheit und Überwachung fest.

EU-Maschinenrichtlinie (Machinery Directive)
Bisherige EU-Richtlinie zur Sicherheit von Maschinen und deren Inverkehrbringen im europäischen Binnenmarkt. Sie definiert grundlegende Sicherheits- und Gesundheitsschutzanforderungen für Konstruktion, Bau und Betrieb von Maschinen. Sie wird 2027 vollständig durch die neue EU-Maschinenverordnung ersetzt.

EU-Maschinenverordnung (Machinery Regulation)
Nachfolgerin der EU-Maschinenrichtlinie. Als Verordnung gilt sie unmittelbar in allen Mitgliedstaaten und enthält aktualisierte Anforderungen an Sicherheit, Digitalisierung und den Einsatz von KI in Maschinen. Sie legt u.a. Pflichten für Hersteller fest und berücksichtigt die Interaktion mit dem EU-AI-Act.

General-Purpose AI
KI-Systeme, die nicht nur für einen einzelnen spezifischen Zweck entwickelt wurden, sondern in verschiedenen Anwendungen und Kontexten einsetzbar sind. General-Purpose AI zeichnet sich durch eine breite Funktionalität aus und kann sowohl allgemeine Aufgaben (z.B. Textverarbeitung, Bilderkennung oder Sprachinteraktion) als auch spezialisierte Anwendungen in unterschiedlichen Branchen abdecken.

Interne Fertigungskontrolle
Ein Verfahren der Konformitätsbewertung, bei dem der Hersteller eigenverantwortlich erklärt, dass ein Produkt die geltenden gesetzlichen Anforderungen erfüllt. Im Rahmen der EU-Maschinenverordnung bedeutet dies, dass Unternehmen die Übereinstimmung ihrer Maschine mit den relevanten Sicherheits- und Gesundheitsschutzanforderungen selbst prüfen und dokumentieren dürfen.

Glossar

ISO/IEC 42001
Internationale Norm für das Management von KI-Systemen. Ziel ist, dass Organisationen KI verantwortungsvoll, sicher und nachvollziehbar einsetzen – inklusive Governance-Strukturen, Risikomanagement, Transparenz und Stakeholder-Einbindung. Besonders relevant ist die Norm für Unternehmen, die KI-Systeme in sicherheitskritischen Bereichen entwickeln oder betreiben.

KI-Reallabor (AI Regulatory Sandbox)
Eine Testumgebung, in der KI-basierte Technologien – wie autonome Inspektionsroboter – unter realen Bedingungen erprobt werden können. Dabei arbeiten Unternehmen, Behörden und Forschungseinrichtungen zusammen, um technische, rechtliche und sicherheitsrelevante Aspekte frühzeitig zu klären. Reallabore ermöglichen eine risikobewusste Erprobung vor dem breiten Markteinsatz.

Konformitätsbewertung
Verfahren zur Prüfung, ob ein Produkt oder ein System die regulatorischen Anforderungen erfüllt (z.B. gemäss EU-KI-Verordnung oder EU-Maschinenverordnung). Je nach Risikoklasse kann es durch interne Prüfungen, externe Audits oder benannte Stellen erfolgen.

LIDAR (Light Detection and Ranging)
Ein optisches Messverfahren zur präzisen Abstandsmessung und Umfelderfassung. LIDAR-Systeme senden Laserimpulse aus und messen die Zeit, bis das Licht von Objekten reflektiert wird. Aus diesen Daten lassen sich dreidimensionale Karten der Umgebung erstellen. In der Robotik dient LIDAR insbesondere zur Navigation, zur Hinderniserkennung und zur Kartierung (z.B. im Rahmen von SLAM).

Notifizierte Stelle
Eine unabhängige, offiziell benannte Prüforganisation, die bestimmte Produkte auf ihre EU-Konformität bewertet. Bei autonomen Inspektionsrobotern mit sicherheitsrelevanter KI-Funktion (z.B. Hindernisvermeidung) ist ihre Einschaltung erforderlich, wenn eine Selbstzertifizierung gemäss EU-Maschinenverordnung nicht zulässig ist.

Reinforcement Learning (bestärkendes Lernen)
Ein Teilgebiet des maschinellen Lernens, bei dem ein KI-System durch gezielte Interaktion mit seiner Umgebung lernt, bestimmte Aufgaben optimal auszuführen. Im Kontext von autonomen Robotern wird Reinforcement Learning zur Steuerung der Lokomotion eingesetzt: Der Roboter lernt, wie er sich stabil und effizient auf komplexem Terrain fortbewegt – etwa durch Treppensteigen oder das Umgehen von Hindernissen.

SLAM (Simultaneous Localization and Mapping)
Ein Verfahren aus der Robotik und der Computer Vision, das es einem mobilen System ermöglicht, sich gleichzeitig in einer unbekannten Umgebung zu orientieren (Lokalisierung) und eine Karte dieser Umgebung zu erstellen (Mapping). SLAM wird typischerweise mit Sensoren wie LIDAR oder Kameras realisiert und ist zentral für die autonome Navigation ohne externe Referenzsysteme wie GPS.

Supervised Learning
Ein Verfahren des maschinellen Lernens, bei dem ein Modell aus gekennzeichneten Trainingsdaten lernt, bestimmte Muster zu erkennen oder Vorhersagen zu treffen. Bei autonomen Robotern wird Supervised Learning eingesetzt, um visuelle, thermische und akustische Inspektionsdaten auszuwerten – bspw. zur Erkennung von Anzeigewerten, ungewöhnlichen Geräuschen oder Temperaturabweichungen an Maschinen.

Autoren

Stephanie Volz
Geschäftsführerin ITSL,
Universität Zürich

Raphael von Thiessen
Programmleiter KI-Sandbox,
Kanton Zürich

Sven Kohlmeier
Fachanwalt für IT-Recht (DE),
Wicki Partners AG

Fallbeispiele aus der Innovation-Sandbox für Künstliche Intelligenz (KI)
Als Fallbeispiel diente das Unternehmen ANYbotics mit seinem autonomen Inspektionsroboter ANYmal. ANYbotics hat im Sommer 2024 einen Projektvorschlag in die Sandbox eingereicht.
Die Inhalte des vorliegenden Reports wurden basierend auf diesem konkreten Fallbeispiel erarbeitet.

Impressum

Herausgeber
Standortförderung, Kanton Zürich
Verein Metropolitanraum Zürich
Innovation Zurich

Projektkonzeption und -koordination
Raphael von Thiessen
Standortförderung Kanton Zürich
8090 Zürich
raphael.vonthiessen@vd.zh.ch

Konzeption in Zusammenarbeit mit
Stephanie Volz
Isabell Metzler
Patrick Arnecke
Markus Müller

Autoren
Raphael von Thiessen
Stephanie Volz
Sven Kohlmeier

Gestaltung
here we are gmbh, here-we-are.ch

Publikation
Dieser Report erscheint ausschliesslich digital und in den Sprachen Deutsch und Englisch.

Projekt-Steering
- Amt für Wirtschaft, Kanton Zürich
- Statistisches Amt, Kanton Zürich
- Staatskanzlei Kanton Zürich
- Amt für Wirtschaft, Kanton Schwyz
- Metropolitanraum Zürich
- ETH AI Center
- Center for Information Technology, Society, and Law (ITSL), Universität Zürich
- swissICT
- ZHAW entrepreneurship