

# Autonomous inspection robots

## *Approaches to the AI Act and EU machinery legislation*

Production facilities in sectors such as energy, oil, gas, nuclear technology and electricity supply are essential for the economy and society. Technical failures can have serious consequences – for safety, the environment and security of supply. Regular inspections are therefore essential; however, they are often time-consuming and hazardous. In addition, fewer and fewer specialists are available to carry them out. Autonomous inspection robots offer a promising solution. They can collect large amounts of data around the clock, analyse it using artificial intelligence (AI) and perform numerous tasks independently. This eases the burden on specialists, avoids hazardous operations and increases operational safety. However, the use of such systems raises complex regulatory issues. Since the EU AI Act came into force, many Swiss robotics companies have faced the question of how to comply with this legislation and other relevant EU requirements such as the Machinery Regulation. As part of the Innovation Sandbox for AI and based on a use case by ANYbotics, the Office for Economy of the Canton of Zurich and the Center for Information Technology, Society, and Law (ITSL) at the University of Zurich have developed strategies for dealing with regulatory requirements for autonomous inspection systems. The findings are intended to support further robotics companies and facilitate access to the EU market.

### ***Innovation Sandbox for AI***

The project team drew up this document as part of the Innovation Sandbox for AI. The Sandbox is a test environment for implementing AI projects from various sectors. This broad-based initiative from government, business and research promotes responsible innovation by ensuring the project team and participating organisations work together closely on regulatory issues and enable the use of

new data sources. The contents of this report are not legally binding and do not represent the official position of any public institutions. Any liability for legal aspects is excluded.

[More information](#)

## Table of contents

---

01.

*Potential of  
autonomous  
inspection robots*

*Page 5*

03.

*Sandbox project  
with ANYbotics*

*Page 19*

05.

*Glossary*

*Page 37*

02.

*Relevant EU  
regulations*

*Page 7*

04.

*Conclusion  
and outlook*

*Page 35*

With expert support from

---

***Dr Ann-Katrin Michel***

*Head of Technology, Swissmem*

***Barbara Mullis***

*Standardisation Expert, Electrosuisse*

***Dr Christian Gehring***

*Co-Founder and Sr. Director of Robotics & AI, ANYbotics*

***Dr Clara Guerra***

*Director, Office for Digital Innovation, Principality of Liechtenstein*

***Elena Maran***

*Global Head of Responsible AI, Modulos AG*

***Jonas Büchel***

*Legal Advisor, Wicki Partners AG*

***Kateryna Portmann***

*Senior Product Manager, ANYbotics*

***Kevin Schawinski***

*Co-Founder and CEO, Modulos AG*

***Marcel Fehr***

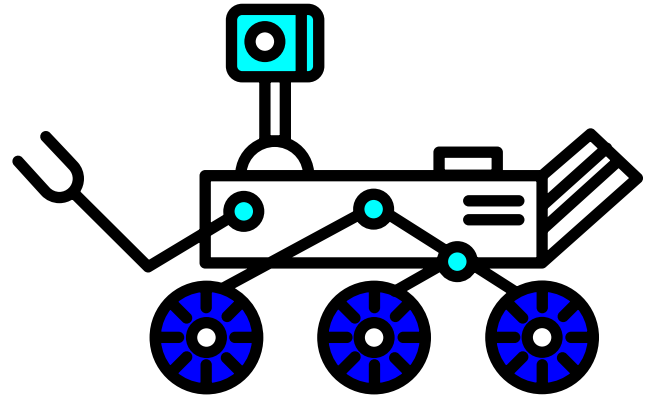
*Senior Certification Manager, ANYbotics*

***Yvonne Finger***

*Head of Unit, Federal Network Agency*

# 01.

## *Potential of autonomous inspection robots*



Industrial plants in sectors such as energy, oil and gas, electricity supply, and chemicals are among the most complex and safety-critical infrastructures in our society. A single outage can have far-reaching consequences – for security of supply, the environment or the staff working on site. To prevent malfunctions, regular inspections are essential. In many cases, these are done manually and in analogue form. Employees perform visual checks, read measuring instruments or record observations on site. Systematic, continuous data collection rarely takes place, which means a basis for predictive maintenance and precise error analysis is often lacking. At the same time, the inspections are very demanding. They lead personnel into confined spaces, onto tall structures or into potentially explosive zones. The physical strain is considerable, and the risk of accidents is real. According to the International Labour Organization, around 395 million workers worldwide sustain a non-fatal occupational injury each year, a significant proportion of which are attributable to hazardous industrial environments. In addition, there is a structural shortage of specialists: Many organisations in the energy sector have difficulty finding enough qualified staff to ensure their operations in the long term. Against this backdrop, autonomous inspection robots are becoming increasingly important. Modern systems can monitor facilities around the clock, record data and carry out initial evaluations without endange-

ring people. These robots are based on a combination of sensors, AI, mobile robotics and *digital twins*. They record temperature, noise, leaks, visual changes or vibration patterns – and automatically determine maintenance requirements or potential hazards. Many of these systems are designed to work alongside humans: They perform routine inspections, capture data from hard-to-reach areas or provide control room staff with real-time data. This reduces the physical presence of people on site and also improves the quality of decisions.

*«Autonomous inspections will be crucial for safety and efficiency in industry in the future.»*

*Raphael von Thiessen,  
AI Sandbox Programme Manager*

\* The terms marked in blue are explained on page 37 in the glossary.

<sup>1</sup> International Labour Organization (ILO), Occupational Safety and Health ([Link](#)).

<sup>2</sup> International Energy Agency, World Energy Employment 2023 ([Link](#)).

# 01. Potential of autonomous inspection robots

---

## **Key benefits of autonomous inspection robots:**

- **Improved safety**  
People are not exposed to hazardous situations.
- **Better underlying data**  
Continuous, standardised recording and transmission improves the quality of data.
- **Greater efficiency**  
Automated routine tasks relieve staff and reduce downtime.
- **Less burden on specialists**  
Personnel shortages are alleviated, as fewer on-site deployments are required.
- **Future viability**  
Integration into digital systems and twins creates new automation potential.

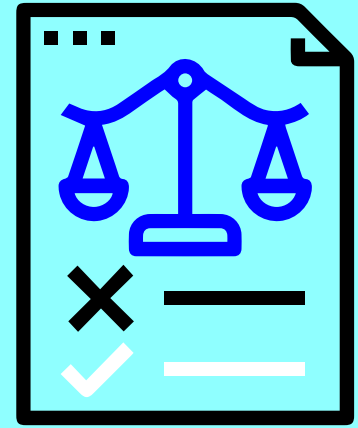
Despite these benefits, there are also some challenges: Autonomous systems might capture incorrect data or misinterpret analyses – especially in complex environments or if sensor values are unclear. Movement malfunctions or unexpected interactions with staff can also pose safety risks – especially in environments that are difficult to navigate. Technical and organisational safety concepts, ongoing quality assurance and a clear division of responsibilities between human and machine are therefore required in order to unlock the full potential of these technologies.

New regulatory issues are also emerging: While the legal framework for machinery (e.g. in the area of product safety) has been established in the EU for years, the use of AI is giving rise to new uncertainties. AI systems that are designed to make decisions or identify risks autonomously raise questions of transparency, accountability and liability. With

the [AI Act](#), a specific regulatory framework for AI has been created in the EU for the first time; however, its interplay with existing EU regulations such as the [Machinery Directive](#), the [Machinery Regulation](#), the [Data Act](#) and the [Cyber Resilience Act](#) poses additional challenges for manufacturers and operators. Careful delineation and combination of the regulatory requirements is necessary, especially for systems that are classified as both machinery and AI application.

# 02.

## *Relevant EU regulations*



Since the introduction of autonomous inspection systems for safety-critical infrastructures such as energy, industrial and transport facilities, Swiss robotics manufacturers have been faced with increasingly complex regulatory issues. EU legislation such as the AI Act, the Machinery Regulation, the Data Act and the Cyber Resilience Act create new frameworks with requirements that not only overlap but also complement or contradict one another. Systems with integrated AI components are affected in particular – in other words, machinery that not only performs mechanical tasks but also analyses and evaluates aspects or prepares and makes decisions on the basis of data.

This chapter provides a structured introduction to the EU regulations that are relevant to such systems. The aim is to present the regulatory basis in a concise way, provide guidance, and outline strategies for legal classification and implementation – particularly for manufacturers based in Switzerland who want to market their products in the EU.

Chapter 3 expands on these principles using a specific practical example from the Canton of Zurich's Innovation Sandbox for AI. The project used ANYmal, a four-legged inspection robot from ANYbotics, to systematically address key regulatory issues relating to the interaction of AI and robotics. The courses of action and strategic considerations developed are not only important for ANYbotics, but also have high practical relevance for other robotics

companies in Switzerland that develop or sell similar systems.

### **2.1 EU Machinery Directive and Machinery Regulation**

In most cases, inspection robots will qualify as machinery regardless of their level of autonomy and will therefore be subject to the applicable legal requirements. The relevant legislation in this context is the Swiss Machinery Ordinance, which is based on the EU Machinery Directive (EC Directive 2006/42/EC) and transposes its requirements into Swiss law.

#### ***What do machinery manufacturers have to bear in mind today if they want to place machinery on the market in the EU?***

If manufacturers want to place an inspection robot on the EU market, they must comply with the provisions of the EU Machinery Directive. A **conformity assessment** stating that the machinery meets all the relevant requirements is required. The CE marking must then be affixed as proof of conformity with all relevant legal provisions.

Switzerland has concluded a Mutual Recognition Agreement (MRA) with the EU for conformity assessments. The aim of the MRA was to enable uniform conformity assessments in Switzerland and the EU and ensure their mutual recognition, i.e. that a Swiss conformity assessment body could certify

## 02. Relevant EU regulations

---

EU conformity, and vice versa. However, the MRA has not been updated since Switzerland rejected the framework agreement. This means: If a provision included in the MRA is amended or replaced, it falls outside the scope of the Agreement. This also eliminates the need for mutual recognition of equivalence.

The EU Machinery Directive is currently part of the MRA, and Swiss machinery manufacturers still benefit from the mutual recognition of conformity. However, the EU Machinery Directive will be replaced by the new EU Machinery Regulation on 20 January 2027. If the MRA is not updated by then, mutual recognition will no longer apply. Swiss manufacturers will therefore need to have the conformity assessment carried out by a *notified body* in the EU.

### ***When does the EU Machinery Regulation come into force?***

The new EU Machinery Regulation (EU 2023/1230) was published in the EU Official Journal on 29 June 2023 and formally came into force on 19 July 2023. It will apply from 20 January 2027 and replace the previously applicable Machinery Directive 2006/42/EC. As a regulation, it is – unlike a directive – directly applicable in all Member States and does not need to be transposed into national law.

The previous EU Machinery Directive will remain fully applicable until 19 January 2027. Manufacturers are already allowed to work according to the new Regulation, but to place a product on the market in a legally compliant way, they must ensure that the requirements of the old Directive are still met. Depending on when the product is placed on the market, it must meet the requirements of either the EU Machinery Directive or the EU Machinery Regulation. If the timing is unknown, the product should comply with both legal frameworks. In such case, issuing two declarations of conformity may be a solution. The manufacturer can thereby confirm that its product

complies with the EU Machinery Directive if placed on the market before 19 January 2027 or with the EU Machinery Regulation if placed on the market on or after 20 January 2027.

The new EU Machinery Regulation will be binding from 20 January 2027. From that date, machinery may only be placed on the market on the basis of this Regulation. Under EU law, placing on the market means making a product available for the first time for distribution or use. The manufacturing date is irrelevant from a legal point of view.

Machinery that was placed on the market before 20 January 2027 in accordance with the EU Machinery Directive may continue to be used, traded and operated. The new Regulation alone does not require any retrofitting. However, if machinery already placed on the market is substantially modified (e.g. through reconstruction, replacement of the control system or a major change to its functionality), this may be considered a new placing on the market.

### ***What will the EU Machinery Regulation change for autonomous inspection robots?***

The EU Machinery Regulation introduces some important changes for manufacturers of autonomous inspection robots. The extent to which these changes apply depends on which parts of the inspection robot are autonomous. The Regulation contains a definition for autonomous mobile machinery.

The new provisions on conformity assessments are particularly relevant: For some types of machinery, the assessment can no longer be carried out by the manufacturer itself, i.e. self-declaration or *internal production control* is no longer possible. This applies to the machinery listed in Annex I, Part A of the EU Machinery Regulation. According to Annex I, Part A, point 6, this includes ‘machinery that has embedded systems with fully or partially self-evolving behaviour using machine learning approaches

## 02. Relevant EU regulations

---

ensuring safety functions that have not been placed independently on the market, in respect only of those systems'. The changes are therefore particularly relevant for AI components that ensure safety functions.

In the case of an autonomous inspection robot, the definition in Annex I, Part A, point 6 of the EU Machinery Regulation should generally be met, as machine learning is typically used for safety-relevant navigation and obstacle detection functions, such as to avoid collisions in complex industrial environments – functions that have a direct impact on the safe operation of the robot.

The EU Machinery Regulation also explicitly stipulates that the machinery must not become hazardous even in the event of lawful or unlawful access (referred to as protection against corruption, Annex III Part B, point 1.1.9).

Furthermore, separate requirements concerning the monitoring function are established in addition to the other essential health and safety requirements of Annex III that may be applicable (Annex III Part B, point 3.2.4).

### ***What does this mean for previous conformity assessments?***

Machinery correctly placed on the market before 20 January 2027 in accordance with the EU Machinery Directive will continue to be considered legally compliant. Declarations of conformity will remain legally valid even after the cut-off date. After that date, machinery may no longer be placed on the market on the basis of the EU Machinery Directive. The new EU Machinery Regulation will apply and a corresponding EU declaration of conformity will be required.

### ***Which conformity assessment procedures are possible?***

For machinery listed in Annex I, Part A of the EU Machinery Regulation, a conformity assessment procedure by a notified body (i.e. rather than the manufacturer itself) is required. The Regulation lists three possible conformity assessment procedures:

- **EU type-examination**  
The notified body examines a sample of the machinery and assesses each type of machinery.
- **Full quality assurance**  
The manufacturer's quality assurance system is assessed, rather than the product. Because quality assurance is carried out, there is no need to assess the individual products.
- **Unit verification**  
Each individual product is assessed.

## 02. Relevant EU regulations

	EU type-examination	Full quality assurance	Unit verification
<b>Benefits</b>	<ul style="list-style-type: none"> <li>• Clear verifiability of a representative robot model</li> <li>• High degree of legal certainty through external assessment</li> <li>• Suitable for individual systems with stable configuration</li> <li>• No documentation of the quality assurance system required</li> </ul>	<ul style="list-style-type: none"> <li>• Not every robot type needs to be assessed</li> <li>• Suitable for manufacturers with ongoing series production</li> <li>• Flexible for software or model adjustments within defined processes</li> </ul>	<ul style="list-style-type: none"> <li>• Suitable for one-off productions or highly specialised robots</li> <li>• No time-consuming inspection of the machinery on site, as certification is based on documentation</li> </ul>
<b>Disadvantages</b>	<ul style="list-style-type: none"> <li>• Any substantial modification to the model requires a new assessment</li> <li>• Manufacturer must grant the notified body access to the machinery</li> <li>• Time-consuming in the case of frequent updates (e.g. for AI developments)</li> <li>• Limited flexibility for software modifications</li> </ul>	<ul style="list-style-type: none"> <li>• Greater initial effort</li> <li>• More complex internal processes and extensive documentation required</li> <li>• Possible unannounced audits</li> <li>• Potentially less economically attractive for smaller providers</li> </ul>	<ul style="list-style-type: none"> <li>• More complex internal processes and extensive documentation (including of the quality assurance system) required</li> <li>• Potentially less economically attractive for smaller providers</li> </ul>

For autonomous inspection robots with safety-relevant AI, the EU type-examination is usually the most appropriate option for stable systems (see Chapter 3.2). For series production, full quality assurance is suitable. Unit verification is only feasible for a small number of individually configured robots.

### ***What is the conformity procedure for autonomous inspection robots?***

If AI components of the inspection robot are covered by Annex I, Part A, the manufacturer must have the conformity assessment carried out by a notified body before being allowed to affix the CE marking. To this end, they must provide comprehensive technical documentation, including risk assess-

ment records, safety evidence for AI components, and information on the training and validation environment. Depending on the method chosen (e.g. EU type-examination or full quality assurance), the process may take weeks or even months and corresponding costs can be expected – especially for testing procedures, audits and documentation preparation. Close coordination with the notified body is essential.

## 02. Relevant EU regulations

---

### Recommended action

*For manufacturers of autonomous inspection robots, the following steps are recommended:*

- **Check classification according to Annex I, Part A**  
Clarify at an early stage whether safety-relevant AI functions of the robot fall under Annex I, Part A, point 6 of the EU Machinery Regulation.
- **Use the transitional period**  
Implement internal changes and product modifications by 19 January 2027.
- **Choose the conformity assessment procedure**  
In consultation with a notified body, check which procedure is appropriate.
- **Involve a notified body**  
If safety-relevant AI components are involved and an external conformity assessment is therefore mandatory, contact a notified body.
- **Prepare technical documentation**  
Ensure that all documentation is complete – including risk assessment records, safety evidence for AI components, and information on the training and validation environment.
- **Observe cybersecurity requirements**  
Take into account mandatory requirements for the protection against cyberattacks and secure software management.
- **Consider the interplay with the AI Act**  
Take interfaces with the AI Act into account, particularly for safety-relevant, learning systems (see Chapter 2.2).

## 02. Relevant EU regulations

---

### 2.2. EU AI Act

The EU AI Act governs the development, marketing and use of AI systems and applications in the EU internal market and follows a risk-based approach. It distinguishes between unacceptable (and therefore prohibited), high-risk, low-risk and minimal-risk AI systems. At its core, the Act sets out detailed requirements that must be observed by manufacturers, operators and other stakeholders in AI value chains.

#### ***What are the requirements for high-risk systems?***

High-risk AI systems are subject to strict legal requirements under the EU AI Act, as they can potentially have a significant impact on the safety, health or fundamental rights of EU citizens. The main obligations are set out in Articles 8–20 of the EU AI Act. Special provisions apply for specific aspects, such as the risk management system. For example, manufacturers are obliged to implement and document a continuous risk management process to identify, minimise and monitor risks throughout the entire life cycle of the systems. Data quality is also subject to certain requirements: Training, validation and test data must be relevant, representative, error-free and non-discriminatory. Other obligations relate to technical documentation, logging functionality, transparency and human oversight.

#### ***To whom does the EU AI Act apply?***

The EU AI Act covers almost all stakeholders along the value chain of an AI system that is to be placed on the market in the EU or the output of which is intended to be used in the EU. This also includes companies that are not based in the EU. The market location principle applies. In particular, this affects manufacturers, providers and operators from third countries such as Switzerland.

#### ***When will the rules of the EU AI Act start to apply, and what are the transitional periods?***

The legislator is adopting a phased approach for the entry into force of the EU AI Act, with transitional provisions for systems already on the market. Individual provisions, such as the ban on certain AI practices (Art. 5), already entered into force on 2 February 2025.

Additional requirements came into effect on 2 August 2025: Transparency obligations for **general purpose AI**, reporting obligations and penalties. Administrative requirements such as governance rules also came into force at that time.

Most requirements, particularly for high-risk AI systems, will generally apply from 2 August 2026. For the most stringent obligations relating to high-risk AI, there will be a transitional period until 2 August 2027.

#### ***Which cut-off dates are particularly relevant for autonomous inspection robots?***

As autonomous inspection robots are likely to be classed as high-risk systems in many cases, the provisions for these systems are particularly relevant. Article 111 of the EU AI Act provides for transitional periods for high-risk systems already on the market. High-risk systems that are placed on the market before 2 August 2026 and are not substantially modified are not subject to the EU AI Act. For high-risk systems used in public authorities, a transitional period until 2 August 2030 applies. The deadlines do not apply to prohibited systems (see below).

#### ***What counts as a substantial modification to an autonomous inspection robot?***

In order for high-risk systems not to be subject to the EU AI Act, they must be placed on the market or put into service before 2 August 2026 and their

## 02. Relevant EU regulations

---

design must not be substantially modified after this date.

The existence of a substantial modification is further defined in Article 3(23) and EC 128 of the EU AI Act. Modifications are considered substantial if they were not foreseen or planned at the time of the initial conformity assessment and if they impair compliance or lead to a modification of the intended purpose for which the AI system was assessed. According to the Act, even changes to the operating system or software architecture constitute a substantial modification of the intended purpose. By contrast, changes to the algorithm and to performance do not, provided they occur automatically during operation and this adaptability was foreseen by the provider and taken into account in the conformity assessment. In practice, it remains to be seen how these provisions will be interpreted specifically. However, under this broad interpretation, virtually any intervention in the AI system could constitute a substantial modification.

Since this concerns product safety law, the provisions of the EU General Product Safety Regulation could also be referred to for the purpose of interpreting the EU AI Act. According to Article 13(3) of this Regulation, the modification of a product is only substantial if it (1) affects product safety, (2) was not foreseen in the original risk assessment, (3) introduces a new risk or alters an existing one and (4) was not carried out by the consumer. It is therefore relevant whether the change is accompanied by an increase in hazards or risks. In this sense, one could argue that routine changes (e.g. operating system updates) that do not increase the risk, or changes that even reduce the risk, are not substantial modifications. However, it can be assumed that the authorities will apply a rather strict standard and will aim to have a large proportion of AI systems covered by the AI Act.

### ***Are there any other exemptions from the application of the EU AI Act?***

In certain areas, the Act applies only to a very limited extent or not at all. This affects some key economic sectors such as civil aviation, agriculture and forestry, marine equipment and the automotive sector, including autonomous driving. Specific approval regulations already exist for these areas.

The Act also excludes certain systems that serve a military purpose or are related to international law enforcement, as well as systems used for scientific research and development, including all related activities. Systems that assist natural persons in personal activities or are licensed under free and open source licences are also excluded, unless they are prohibited or subject to specific transparency obligations.

In addition, the AI Act does not apply if the personal scope of application has not been met. In particular, a provider may lose its role as a provider if, for example, a distributor, importer or operator places on the market or puts into service an AI system already made available in the EU under its own name or trademark, or makes substantial modifications to the system. This may occur, for example, through a 'white label' sale. It is also conceivable that a provider may transfer an AI system produced in Switzerland to a legal entity in the EU for placing on the market.

### ***Are there any administrative simplifications for smaller manufacturers of autonomous inspection robots?***

Yes, small and medium-sized enterprises (SMEs) and start-ups that have their main place of business or a secondary establishment in the EU and employ fewer than 250 people or have either an annual turnover of up to EUR 50 million or an annual balan-

## 02. Relevant EU regulations

---

ce sheet total of up to EUR 43 million, can benefit from certain administrative simplifications. For example, they have to provide less extensive technical documentation, and the fees for the conformity assessment are also lower. In addition, they are given priority and free access to AI regulatory sandboxes. The size of the company also plays a role in the determination of penalties. In terms of staff training and risk management, however, SMEs are subject to the same requirements as larger companies.

### ***Is an autonomous inspection robot always a high-risk system?***

The EU AI Act defines two different categories of high-risk systems. According to Article 6(1), an AI system is considered high-risk if both of the following conditions (a) and (b) are fulfilled: (a) The AI system is itself a product covered by the Union legislation listed in Annex I or is used as a safety component of a product (e.g. as an AI safety component in machinery) covered by the Union legislation listed in Annex I; and (b) the Union harmonisation legislation requires a third-party conformity assessment before the product is placed on the EU market.

Examples of Union harmonisation legislation include the Machinery Regulation, the Medical Devices Regulation, the Toy Safety Directive and vehicle safety regulations. The relevant legislative acts are set out in Annex I of the AI Act.

For autonomous inspection robots, the applicable Union harmonisation legislation is the EU Machinery Directive (or, at the relevant time, the EU Machinery Regulation). If the autonomous inspection robot uses a safety component with AI or is itself a safety component (which is unlikely to be the case), it is considered a high-risk system if a conformity assessment is required under the EU Machinery Regulation (see Chapter 2.1).

According to Article 3, point 14 of the EU AI Act, a safety component is a part of a product or AI system that performs a safety function for that product or AI system, or the failure or malfunction of which would endanger the health and safety of persons or property. In autonomous inspection robots, the AI system is often located in the control area. It can therefore be assumed that its failure could at least endanger property. Condition a) is therefore fulfilled. In addition, the entire product, i.e. the robot, must undergo a conformity assessment in accordance with the EU Machinery Regulation. Thus, condition b) is also fulfilled. It is therefore very likely that an inspection robot will qualify as a high-risk system within the meaning of Article 6(1) of the EU AI Act. However, this may not be the case, depending on which functions the AI system performs.

In addition, all systems listed in Annex III of the Act are classified as high risk, as they are used in safety-critical areas, including critical infrastructure. According to Annex III, point 2, only AI systems that are intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic or the supply of water, gas, heat or electricity are considered high risk in connection with critical infrastructure. It therefore depends on whether the AI system is a safety component.

This raises the question of whether the AI system or the autonomous robot can be classified as a safety component of the critical infrastructure. Again, the decisive factor is whether a failure of the system would increase the risk to the safety or health of people. Autonomous inspection robots that are only used for data collection (e.g. for visual inspections or condition monitoring) without directly intervening in control or operating processes do not usually have a safety component within the meaning of the AI Act.

## 02. Relevant EU regulations

---

Accordingly, the system does not automatically fall into the high-risk category of Annex III, point 2 of the EU AI Act. The situation is different for AI systems that actively perform safety-relevant functions – such as an AI that controls the flow of electricity in an energy supply system. A safety component is clearly present in this case, which means a corresponding conformity assessment by a notified body is required. A detailed examination of the system's function and use is therefore essential.

### ***Are there any other exemptions from the application of the AI Act?***

In addition, the AI Act does not apply if the personal scope of application has not been met. In particular, a provider may lose its role as a provider if, for example, a distributor, importer or operator places on the market or puts into service an AI system already made available in the EU under its own name or trademark, or makes substantial modifications to the system. This may occur, for example, through a 'white label' sale. It is also conceivable that a provider may transfer an AI system produced in Switzerland to a legal entity in the EU for placing on the market.

## Conformity assessments in accordance with the EU Machinery Regulation and the EU AI Act

### ***When are conformity assessments required under the EU AI Act?***

Conformity assessments are only required for high-risk AI systems. They should demonstrate that the system complies with the requirements of the EU AI Act (e.g. data quality, transparency, risk management, human oversight).

If the high-risk AI system is part of a product subject to other EU harmonisation acts (e.g. a medical device, a machine or a vehicle), an external conformity assessment by a notified body is generally required. The latter must verify conformity and, where appropriate, draw up an EU declaration of conformity. If an AI system passes the conformity assessment, it may carry the CE marking (see Chapter 2.1).

*«AI-based robotics systems show just how complex and comprehensive the requirements of EU law are.»*

*Stephanie Volz, Managing Director ITSL*

## 02. Relevant EU regulations

---

### ***To what extent can an existing conformity assessment under the EU Machinery Directive or Regulation be recognised?***

The EU AI Act states in several places that, in the case of products and AI systems that have already undergone certain conformity assessments under harmonisation legislation, the documents and documentation used for these assessments can also be used for the documentation under the EU AI Act, and the requirements of the EU AI Act can be integrated into the existing documentation.

### ***Do two conformity assessment procedures have to be carried out, i.e. one according to the EU Machinery Regulation and one according to the EU AI Act?***

No, two separate procedures do not have to be carried out. If a product falls under the EU Machinery Regulation, a conformity assessment procedure for this Regulation is applied. Since its requirements largely overlap with those of the EU AI Act (see the checklist for high-risk systems in Chapter 3.2), compliance with the EU Machinery Regulation is mainly checked within this procedure. However, if there is a requirement under the EU AI Act that is not covered by it, that requirement will be assessed in the same procedure by the same notified body.

### ***Does the entire machinery have to undergo a conformity assessment by a notified body, or only part of it?***

The entire robot or machinery does not have to be assessed by the notified body, but rather only those parts that ensure a safety function. In the case of an autonomous inspection robot, this is likely to be the control unit. The remaining parts must be checked by the manufacturer itself and subjected to a conformity assessment.

## 02. Relevant EU regulations

---

### Recommended action

- **Check high-risk classification**  
Carefully check whether the AI system is to be classified as a safety component in accordance with the EU Machinery Regulation or as a high-risk system in accordance with Annex III of the EU AI Act.
- **Take into account transitional periods**  
When planning market entry, bear in mind that systems that are placed on the market before 2 August 2026 and not substantially modified are not subject to the new obligations of the EU AI Act.
- **Assess system modifications**  
When making changes to software, the operating system or system architecture, carry out a careful risk assessment, as they may be considered a substantial modification and therefore require a new conformity assessment.
- **Integrate conformity procedures**  
Combine the conformity assessment required for high-risk systems according to the EU AI Act with the assessment according to the EU Machinery Regulation.
- **Use existing documentation**  
To meet the requirements of the EU AI Act, use the technical documentation from the conformity assessment according to the EU Machinery Regulation.
- **Utilise administrative simplifications for SMEs**  
Take advantage of the administrative simplifications for SMEs under the EU AI Act, including reduced documentation requirements and free access to regulatory sandboxes.
- **Define the role of the provider**  
Transfer the role of the provider to a legal entity based in the EU, if necessary, and thereby shift the regulatory obligations accordingly. This is possible provided it does not constitute prohibited circumvention.

## 02. Relevant EU regulations

---

### 2.3. Other legal acts

In addition to the central regulatory frameworks – the **Machinery Regulation and the AI Act** – there are other regulatory developments at EU level that may also affect autonomous inspection systems:

- **Data Act**

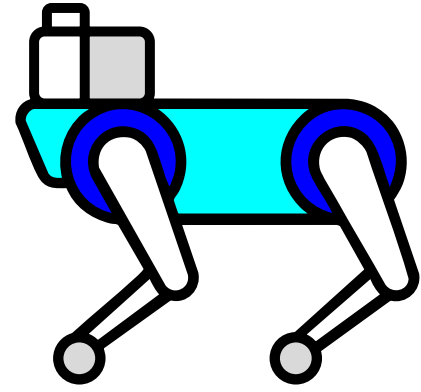
The Data Act establishes a harmonised legal framework for the use, sharing and access to data within the EU. It obliges manufacturers and providers of connected products and related services to make generated data accessible, and governs data exchange between companies (B2B) as well as with public authorities (B2G). For operators of autonomous inspection systems, the provisions on data portability, access rights and contractual transparency are particularly relevant.

- **Cyber Resilience Act**

The Cyber Resilience Act introduces horizontal cybersecurity requirements for all digital products with connected functionality. Manufacturers must demonstrate security-by-design and security-by-default, implement vulnerability management, and ensure security updates throughout the entire product lifecycle. For autonomous inspection systems, this entails stricter requirements for secure software development, patch management, and proof of corresponding processes as part of the conformity assessment.

# 03.

## *Sandbox project with ANYbotics*



### **3.1. ANYmal use case**

As part of the Innovation Sandbox for AI, the product ANYmal served as a use case to clarify regulatory requirements. ANYmal is an autonomous, four-legged inspection robot from the Swiss company ANYbotics, developed for demanding industrial environments such as power plants, offshore platforms and chemical plants. Thanks to its dynamic walking mechanism, it can move stably over uneven terrain, stairs and grids – wherever wheeled or tracked systems reach their limits.

The platform combines three integrated AI components that are usually processed locally on powerful CPU/GPU units:

- **Reinforcement learning for locomotion** adaptive movement in complex environments
- **Self-learning navigation** autonomous route finding and obstacle avoidance
- **Supervised learning for inspections** analysis of visual, acoustic and physical sensor data

ANYmal uses a multimodal sensor system that includes the following components, among others:

- **360°-LIDAR** for **SLAM**-based mapping and navigation
- **Depth and zoom cameras** for visual detection and documentation
- **Thermal imaging camera** for temperature monitoring
- **Acoustic and vibration sensors** for monitoring the condition of machinery

Communication typically runs via Wi-Fi, 5G or edge computing interfaces and is directly connected to digital twins or industrial monitoring systems. The power is supplied via an automatic charging station, which ensures continuous operation.

### **Core functions of ANYmal**

- **Mobile mapping and 3D scanning**  
Capture entire systems in high resolution
- **Sensor integration**  
Temperature, leakage, visual indicators (e.g. level, pressure gauges), noise and vibration
- **Intelligent inspection**  
Automatic adjustment of the sensor position (e.g. camera angle during reflection), additional recordings in the case of uncertainties

# 03. Sandbox project with ANYbotics

- **Real-time data transmission**  
Direct transmission of information to the central monitoring system or to the system’s digital twin
- **Robust design**  
Protection against heat, dust, humidity, explosive environments (*ATEX*-certified version available)

ANYmal is now used in productive environments around the world – from energy supply to the chemical industry. The robot provides support with routine checks, preventive maintenance or emergency operations, for example.



### Example application 1: Chemical plant

In a chemical production plant, the autonomous inspection robot ANYmal is used in regular operation for daily inspection rounds. It inspects over 120 visual, thermal and acoustic inspection points per mission, including temperature displays, pump noise and corrosion characteristics. Deviations are documented and reported automatically. The collected data flows into the system’s digital twin and supports continuous condition monitoring. According to the operator, a measurable increase in plant availability was achieved through use of the system. There are plans to extend it to other sites.



### Example application 2: Offshore platform

On an offshore platform, the autonomous inspection robot ANYmal X is used as part of regular inspection rounds. It checks the visual, thermal and acoustic characteristics of valves, pumps and electrical systems – including in potentially explosive atmospheres with high humidity and changing weather conditions. Inspections are carried out at several levels and in areas that are difficult to access. The collected data is automatically transmitted to the maintenance team and integrated into existing digital systems. According to the operator, the system helps reduce the need for personnel in safety-critical areas and enables continuous monitoring of the plant condition.

## 03. Sandbox project with ANYbotics

---



### Example application 3: Data centre

In a data centre, the autonomous inspection robot ANYmal is used for regular inspection rounds. It monitors visual, thermal and acoustic condition characteristics of technical building installations such as cooling, power supply and cabling – even in poor lighting conditions or at night. The inspection data is automatically recorded and transmitted to the in-house maintenance platform. Deviations are detected and reported to enable timely manual intervention. According to the operator, the use of the system contributes to increasing operational safety and automating recurring test tasks. The robot is in continuous operation and carries out several inspection missions per day.

These three application examples – chemical plant, offshore platform and data centre – illustrate the range of potential applications for autonomous inspection robots in real industrial environments. They show how these kinds of systems can help to complement existing control processes, especially in difficult-to-access or safety-critical areas. At the same time, they make clear which technical, organisational and regulatory issues need to be taken into

account when introducing these types of technologies.

### Practical benefits

- Improved inspection to identify risks and technical problems at an early stage
- Less deployment of personnel in hazardous zones
- Basis for predictive maintenance and long-term cost reduction
- Seamless documentation and improved data quality
- Reduced workload of technicians for repetitive inspection tasks
- Integration into digital twins and existing monitoring systems

### Implementation challenges

- Integration into existing infrastructures and IT systems
- Adaptation of operating procedures to robot-assisted inspection processes
- Personnel training for system operation and maintenance
- Challenging environmental conditions (e.g. extreme heat, humidity)
- Network connectivity for real-time data transmission
- Continuous system calibration and error detection

## 03. Sandbox project with ANYbotics

---

### 3.2. Dealing with EU regulations

The legal classification of autonomous inspection robots poses complex challenges for manufacturers and regulators. In particular, the interface between the EU AI Act and the EU Machinery Regulation raises key questions: Under what conditions should such systems be classified as high-risk AI systems (HRAIS) (see Chapter 2.2)? What obligations arise for manufacturers, and what opportunities emerge from different interpretations? Using the example of the ANYmal robot (see Chapter 3.1), the following chapter analyses possible strategies for dealing with regulatory requirements. Two scenarios are compared. In the first scenario, the robot is not classified as a HRAIS, while in the second it is. In this case, the stricter requirements are implemented proactively.

In the first scenario, it is argued that the inspection robot should not be classified as a HRAIS. The advantage of this approach is that systems not considered high risk have to meet less stringent requirements. The disadvantage is that the arguments against classifying the system as a HRAIS are, in this case, not very robust. If the matter were to be assessed by an authority or a court, there is a risk that they could reach a different conclusion. The robot would then have to be certified according to the newly introduced conformity assessment procedure of the EU AI Act. This procedure has not yet been established by the responsible inspection bodies ('notified bodies'), which, from the Sandbox team's perspective, may lead to uncertainty, more work and higher certification costs.

In the second scenario, it is argued that the robot is a HRAIS. In this case, the manufacturer must implement the corresponding requirements of the EU AI Act. The advantage of this strategy is that the robot cannot be certified via the new conformity assessment procedure of the EU AI Act, but via the already established conformity assessment procedure of the EU Machinery Regulation. This procedure is more established among notified bodies (with the exception of the requirements of the EU AI Act), which results in less uncertainty and lower costs. The disadvantage is that HRAIS have to meet more stringent requirements than low-risk systems.

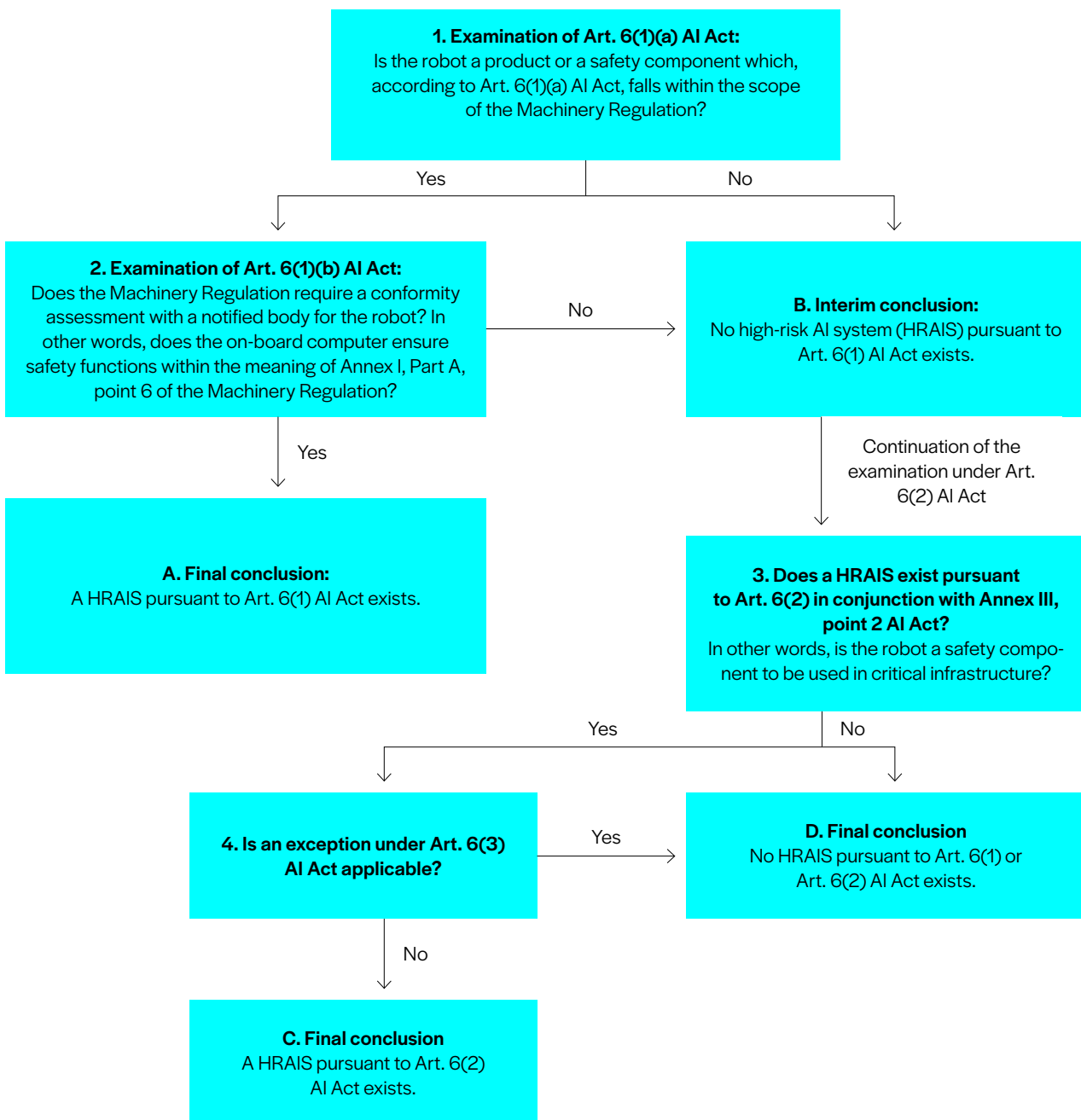
*«For ANYbotics, the implementation of various EU regulations is key to market access.»*

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

# 03. Sandbox project with ANYbotics

## I. Scenario 1: not classified as HRAIS

Scenario 1 includes several options to avoid the robot being classified as a HRAIS. They are shown in a decision tree that leads step by step through the relevant checks. The starting point is the analysis of the requirements under Article 6(1) of the EU AI Act, followed by the assessment under Article 6(2). This is followed by an explanation of the decision paths which, from the sandbox team's perspective, offer a reasonable basis for not classifying the robot as a HRAIS.



## 03. Sandbox project with ANYbotics

---

### **Option 1: No safety component**

A viable approach within the first scenario is derived from the following path in the decision tree:

#### **1. Yes, 2. No, 3. No → D**

First, it must be checked whether the robot is a product or a safety component according to Article 6(1)(a) of the EU AI Act and falls under the EU Machinery Regulation. The sandbox team assumes that this is the case, as ANYbotics has already assessed the robot under the previous EU Machinery Directive. However, this assumption has not been examined in detail. It should be noted that the conditions set out in points (a) and (b) of Article 6(1) of the EU AI Act must be met cumulatively. Therefore, if the robot is not a safety component or a product referred to in point (a), it is no longer necessary to check whether it needs to undergo a conformity assessment under point (b). However, since it is very likely that point (a) is met for ANYmal, it must be checked whether point (b) is also met.

The sandbox team argues that the robot is not subject to a conformity assessment under the EU Machinery Regulation and that Article 6(1)(b) of the EU AI Act is therefore not fulfilled. According to Article 25(2) of the EU Machinery Regulation, those products listed in Annex I, Part A are subject to a conformity assessment. In this Annex, point 6 is particularly relevant for the robot. However, point 6 requires the robot to have an ‘embedded system’ that ensures safety functions. According to Article 3(4) of the EU Machinery Regulation, a safety function is a function that serves as a protective measure to eliminate or reduce a risk and the failure of which would lead to an increase in the risk. However, the embedded system installed in the robot, the on-board computer, does not ensure safety functions according to this definition. This is justified by the fact that it is not currently possible to verify the safety of a machine learning method – such as that used

for the obstacle avoidance system – for technical reasons. Thus, if it is not clear how safe the obstacle avoidance system is, it does not guarantee a safety function. The same applies to the Locomotion and Inspection Intelligence modules. Since the conditions of points (a) and (b) must be met cumulatively, the answer ‘No’ at this stage leads to the conclusion that no HRAIS exists within the meaning of Article 6(1) of the EU AI Act.

However, a HRAIS in accordance with Article 6(2) and Annex III, point 2 of the EU AI Act could exist. For this to be the case, the robot would have to be a safety component of a critical infrastructure. The sandbox team argues that the robot is not considered a component because there is no fixed connection to critical infrastructure. As already mentioned, it does not perform any safety functions either. This leads to the conclusion that the robot is not to be classified as a HRAIS under either Article 6(1) or Article 6(2) of the EU AI Act.

### **Option 2: Exemption under Article 6(3) of the EU AI Act**

An alternative decision-making process can be found via the following path:

#### **1. Yes | 2. No | 3. Yes | 4. Yes → D**

Here, the sandbox team assumes, with the same reasoning as for Option 1, that no HRAIS under Article 6(1) of the EU AI Act exists. On the other hand, it is assumed that the robot is a safety component of a critical infrastructure. The reasoning is that failure of the robot could result in an increased risk to the safety of people, so a safety component within the meaning of Article 3, point 14 of the EU AI Act is therefore present. In addition, it is argued that the term ‘safety component’ is not only to be interpreted literally, so that a non-fixed system such as the robot can also be considered a component. Thus, a HRAIS pursuant to Article 6(2) of the EU AI Act exists.

## 03. Sandbox project with ANYbotics

---

Finally, the exemptions under Article 6(3) of the EU AI Act need to be examined. If one of these exemptions applies, no HRAIS exists despite the conditions of Article 6(2) of the EU AI Act being met. Here, it is argued that the robot does not make independent decisions, but rather only performs preparatory activities for human decision-makers. Therefore, the exemption provided for in Article 6(3)(d) of the EU AI Act is relevant and no HRAIS exists. Overall, this path also leads to the conclusion that the robot is not to be classified as a HRAIS under either Article 6(1) or Article 6(2) of the EU AI Act.

### **Option 3: Use of transitional provisions**

A third option within the first scenario is to invoke the transitional provisions of the EU AI Act. According to Article 111, the EU AI Act does not apply to AI systems already on the market if they were placed on the market or put into service before 2 August 2026, unless there is a substantial modification to the design. However, it remains unclear what is meant by a substantial modification. The EU AI Act defines a 'substantial modification' as a change that was not foreseen or planned in the original conformity assessment carried out by the provider, and that either affects the conformity of the AI system or results in a change to the intended purpose for which the system was assessed. A substantial modification therefore only exists if compliance with the EU AI Act is no longer ensured as a result of the change. In line with established practice under the EU Machinery Directive, the key consideration is whether the change gives rise to a new hazard or increases an existing risk to the legal interests protected by the EU AI Act.

*«EU regulations often have a less drastic impact on companies than expected – those who make smart use of flexibilities and analyse risks pragmatically can develop a suitable strategy.»* Sven Kohlmeier,  
Specialist Attorney for IT Law,  
Wicki Partners AG

## 03. Sandbox project with ANYbotics

---

### Conclusion for the first scenario

This scenario offers the possibility of avoiding the robot being classified as a HRAIS. However, whether the corresponding argument would stand up to judicial review is currently open, as there is not yet any case law on these issues. Against the backdrop of geopolitical competition, particularly with regard to technological competition from the US, a broad interpretation of the EU AI Act by the EU could be promoted. If the robot is not classified as a HRAIS, it is not subject to a conformity assessment procedure according to the EU AI Act and only needs to comply with the Act's general requirements for AI systems. However, a conformity procedure according to the EU Machinery Regulation may still be necessary. In addition or as an alternative to arguments against classification as a HRAIS (Options 1 and 2), the transitional provision (Option 3) may be invoked to temporarily avoid the application of the EU AI Act.

### II. Scenario 2: Classification as a HRAIS

In this scenario, it is assumed that the robot will be subject to the new EU Machinery Regulation and will have to be certified by a notified body. As this fulfils the conditions of Article 6(1)(a) and (b), a HRAIS exists.

Certification according to EU Machinery Regulation  
In the case of a HRAIS, the sandbox team recommends that the manufacturers first carry out the conformity assessment procedure according to the EU Machinery Regulation. The notified body simultaneously verifies compliance with the requirements of the EU AI Act. Certification according to the EU AI Act is therefore not required. In this way, manufacturers only have to go through the established procedure. The potentially more expensive, new procedure under the EU AI Act can be avoided.

The decisive factor is that, according to the EU Machinery Regulation, it is not the entire robot that has to be certified, but rather only the on-board computer, i.e. the control unit in which the AI functions are embedded. Certification is required for 'embedded systems with self-developing behaviour', the failure of which would increase the risk to persons. Accordingly, based on discussions with the manufacturer, the following robot modules in particular could be subject to certification:

- **Obstacle avoidance**  
An outage could lead to accidents.
- **Inspection intelligence**  
A defect could give rise to risks (e.g. unnoticed leaks).
- **Locomotion**  
An error could cause the robot to fall and thus create a hazard.

## 03. Sandbox project with ANYbotics

---

Three procedures are available for the certification of the on-board computer (see Chapter 2.1):

**1. EU type-examination**

The most suitable; a single model is tested, no ongoing audits

**2. Full quality assurance**

Unsuitable due to unannounced audits

**3. Unit verification**

Unsuitable for series production due to high costs

The other components of the robot, such as legs or housing, can continue to be verified through internal production control.

The reasoning in the second scenario requires only one certification by a notified body – namely according to the EU Machinery Regulation. Conformity with the EU AI Act is checked at the same time. Only the on-board computer needs to be certified externally, while the rest of the robot can be tested internally. The most appropriate conformity assessment procedure for ANYbotics is the EU type-examination. Furthermore, the obligations for HRAIS providers under the EU AI Act must be observed. The advantages of the second scenario are reduced legal risk and established procedures. The disadvantage is that stricter requirements have to be met than in the first scenario.

### Conclusion for the second scenario

## Recommended action

The decision between the different argumentation scenarios is not only a legal one – it also requires business judgement. If the robot is subject to the EU Machinery Regulation anyway, the sandbox team recommends choosing the implementation strategy from Scenario 2, going through the certification procedure under the EU Machinery Regulation – ideally in the form of EU type-examination – and thus meeting the requirements of the EU AI Act at the same time.

## 03. Sandbox project with ANYbotics

### Checklist for high-risk systems

The EU AI Act imposes a number of obligations on providers of HRAIS. The EU Machinery Regulation contains obligations for manufacturers of machinery that are congruent or similar (see fourth column). Therefore, by going through the conformity assessment procedure under the EU Machinery Regulation, some obligations under the EU AI Act are already fulfilled at least in part. Here is a checklist of all obligations that the EU AI Act imposes on providers of HRAIS:

Completed	Obligation	Articles in the EU AI Act	Similar obligation under the EU Machinery Regulation
☐	Indicating name, trademark and contact address	16 b)	10 VI
☐	Establishing a quality management system	16 c), 17	For full quality assurance: Annex IX, point 3; in the case of individual verification: Annex X, point 2, sub-paragraph 3 ii)
☐	Preparing and retaining documentation	16 d), 11, 17, 47, 18	10 II, Annex IV Part A
☐	Retaining automatically generated logs for 6 months	16 e), 12, 19	Annex III, Part B, point 1.2.1. Sub-paragraph 3 b): Retention period of 1 year
☐	Carrying out a conformity assessment procedure (in the case of ANYbotics, according to the EU Machinery Regulation)	16 f), 43 III, Regulation (EU) 2023/1230	10 II, 25
☐	Drawing up an EU declaration of conformity	16 g), 47	10 II
☐	Affixing a CE marking	16 h), 48	10 II
☐	Taking corrective measures if the HRAIS is not (or no longer) compliant with the EU AI Act after it has been placed on the market	16 j)	10 IX
☐	If requested by the authorities: demonstrating compliance with requirements for HRAIS	16 k), 8–15	10 X
☐	Establishing a risk management system	9	Annex IV, Part A (b): Risk assessment
☐	Creating technical documentation that contains information in accordance with the EU AI and EU Machinery Regulation	11, Annex IV, Regulation (EU) 2023/1230	Annex IV Part A
☐	Creating an operating manual that enables transparent operation	13	10 VII
☐	Ensuring human oversight	14	Annex III, Part B, point 3.2.4.
☐	Ensuring sufficient accuracy, robustness and cybersecurity	15	Annex III, Part B, point 11.9: Protecting against corruption
☐	Ensuring accessibility of websites and products	16 l), Directive (EU) 2016/2102, Directive (EU) 2019/882	
☐	Establishing a data governance process to ensure that training data is as error- and bias-free as possible	10	
☐	Establishing a post-market monitoring system for the HRAIS (ANYbotics customers must forward data for this purpose)	72	
☐	Reporting serious incidents to the market surveillance authority	73	
☐	If required by the authority: conformity with EU AI Act verified by market surveillance authority	79, Regulation (EU) 2019/1020	
does not apply	Registering in the EU database for HRAIS according to Annex III (ANYbotics does not fall under Annex III)	16 i), 49, 71, Annex III	

## 03. Sandbox project with ANYbotics

---

### 3.3. AI governance and ISO/IEC 42001

Regardless of whether an autonomous inspection robot is classified as a HRAIS in regulatory terms, systematic AI governance is becoming increasingly important. Regulatory requirements in the areas of AI, cybersecurity, product safety and data access will continue to grow in the coming years – both in the EU and globally.

Structured governance makes it possible to take into account existing and future requirements in a targeted manner without having to develop a separate approach for each new regulatory instrument. This is because a centrally anchored AI management system can map various regulatory requirements – such as those from the EU AI Act, but also AI-related requirements from the EU Machinery Regulation or AI regulations in other regions that are of interest as a market.

The following section presents a possible implementation approach for such AI governance based on *ISO/IEC 42001*.<sup>3</sup> This international standard defines, for the first time, a structured management system specifically for the responsible use of AI. It builds on established principles of information security and quality management and applies them to AI-specific risks and control processes. The concept of an AI management system was tested in practice as part of the sandbox project with ANYbotics in collaboration with Zurich-based company Modulos AG. The aim was to prepare a lean system that addresses regulatory requirements in a structured manner and at the same time provides a modular basis for specifically filling regulatory gaps where necessary (e.g. from the EU AI Act or the EU Machinery Regulation). The experience gained from the use case was incorporated – particularly with regard to system delimitation, organisational anchoring and selected documentation and control tools.

*«Those who systematically embed AI governance create security, reduce risks and secure long-term market access.»* Elena Maran,  
Global Head of Responsible AI, Modulos AG

#### Motivation and objectives

The aim was to prepare for the introduction of an AI management system in accordance with the requirements of ISO/IEC 42001 – as a first concrete step towards establishing AI governance in the company. This was done against the background that there is still no final legal clarity regarding the interaction between the EU AI Act and the EU Machinery Regulation. The decision to introduce an AI management system was motivated by several interrelated factors. On the one hand, ANYbotics is active in highly regulated industries – including oil and gas, mining, chemicals, and power generation – and operates in more than 20 countries. On the other hand, AI technologies are an essential part of the company's product, and compliance with regulatory requirements is becoming increasingly important – especially with regard to the potential classification of autonomous robot systems as high-risk applications under the EU AI Act. In addition, customer requirements in terms of AI governance and the desire for competitive and responsible AI development have supported the

<sup>3</sup> See ISO 42001:2023 'Information technology – Artificial intelligence – Management system' (available as the identical Swiss standard SN ISO/IEC 42001:2025 at: <https://connect.snv.ch/de/sn-isoiec-42001-2025>). Manufacturers are advised to use the standard early on as an orientation framework for establishing an AI management system and to align it with existing quality and safety standards.

## 03. Sandbox project with ANYbotics

---

ambition to establish a comprehensive AI governance framework. At the same time, an implemented AI management system also increases customer trust.

### **Technical challenges and regulatory complexity**

During the preparation of the AI management system at ANYbotics, some challenges arose that are typical of AI-supported robotics systems in industrial environments. The following points are particularly relevant:

- **Autonomous navigation in safety-critical environments**  
The use of ANYmal in facilities such as refineries, chemical plants or power plants is subject to strict safety requirements. Faulty navigation or wrong decisions by AI can have serious consequences in such contexts.
- **Integration of third-party AI components**  
External AI modules are sometimes used for central functions such as image processing. The validation, traceability and long-term maintenance of such components are particularly challenging – especially with regard to regulatory requirements.
- **Model drift under real operating conditions**  
Different lighting conditions, structural changes in facilities, weather conditions or contamination can change the performance of AI models in the field. The stability and robustness of the models must therefore be continuously monitored and tested.
- **Regulatory diversity across more than 20 countries of operation**  
ANYbotics operates internationally and must comply with regulatory requirements from different jurisdictions. Ensuring compliance with the EU AI Act, the EU Machinery Regulation and other national regulations is a significant challenge.

- **High update frequency and version control**  
The system is updated in quarterly cycles. This requires stringent processes for versioning, test documentation, release and traceability – especially in the case of safety-critical components.

The ANYmal robot system combines advanced AI such as deep learning or reinforcement learning with generative AI for computer vision, navigation and inspection. It is precisely this technical complexity that underscores the need for a structured, risk-based approach to AI governance – both to meet regulatory requirements and to ensure safety, quality and scalability in operations. The existing information security management and safety structures were an important basis for addressing AI-specific risks with independent, specialised governance structures.

### **Risk assessment**

The risk analysis revealed a medium risk for ANYbotics, which is shaped by the complex regulatory environment, the autonomous use of the systems and the technological complexity of the AI components. Although the existing information security management system and established risk management processes reduce vulnerability, there is still some scope for development, particularly with regard to developing dedicated resources for AI governance.

# 03. Sandbox project with ANYbotics

Overall risk assessment Moderate		
<b>External</b> <b>Assess regulatory context</b> <ul style="list-style-type: none"><li>• EU AI Act (potential high-risk classification)</li><li>• Compliance in multiple jurisdictions</li><li>• Dynamic/ongoing regulatory developments</li></ul>	<b>Operational</b> <b>Assess operational use</b> <ul style="list-style-type: none"><li>• Limited human oversight during operation</li><li>• Real-time decision-making</li><li>• Safety-critical environments</li></ul>	<b>Technical</b> <b>Assess system autonomy</b> <ul style="list-style-type: none"><li>• Reliability and robustness challenges</li><li>• Lack of transparency of reinforcement learning systems</li><li>• Model drift and data quality</li></ul>

## Main AI risks

The comprehensive risk analysis identified 10 critical risks, which are divided into three interrelated categories.

- 1. External risks** focus on the complex regulatory environment and stakeholder management challenges. Difficulties with regulatory compliance result from the constantly evolving AI requirements in various jurisdictions. At the same time, there are risks in relation to stakeholders, particularly when it comes to clearly communicating the capabilities and limitations of AI systems to industry partners, who often operate in risk-averse environments.
- 2. Operational risks** arise from the special requirements for using autonomous systems with real-time decision-making in safety-critical contexts. To avoid potential safety risks, it is essential that the systems can be monitored by humans. Gaps in the overarching AI governance also highlight the need for structured accountability mechanisms. Update management challenges arise from the quarterly roll-out cycle, while runtime risks underscore the vulnerability of autonomous systems to targeted attacks, with potential implications for operational safety and functionality.
- 3. Technical risks** dominate the assessment. They include fundamental challenges related to the reliability and robustness of AI systems in unpredictable industrial environments, as well as the inherent opacity of decision-making processes in complex reinforcement learning systems. A particular concern is the risk of model drift due to the dynamic conditions in inspection environments. In addition, there are challenges in terms of data quality and AI-specific security vulnerabilities, which present ongoing operational hurdles and require targeted countermeasures.

## 03. Sandbox project with 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

### Statement of applicability

The 10 identified risks formed the basis for the selection and prioritisation of the control measures implemented in the AI management system. It was found that many of the technical and operational challenges require specific governance tools. Based on ANYbotics' dual role as a medium-risk AI provider and manufacturer, the Statement of Applicability covers all essential controls from Annex A of ISO/IEC 42001, with the exception of the societal impact assessment (A.5.5). This was excluded due to the limited application context in the area of industrial inspections. The relevant controls focus in particular on:

- **AI policies (A.2)**
- **Governance roles (A.3)**
- **Life cycle management (A.6)**
- **Data governance (A.7)**
- **Responsible use (A.9)**

### Risk-based prioritisation of implementation controls

The prioritisation of controls was based on a medium risk, the dual role of AI provider and manufacturer, the existing information security management structure and the fact that no sensitive personal data is processed. This made it possible to focus specifically on those requirements that are particularly relevant to industrial robotics, such as

# 03. Sandbox project with ANYbotics

system reliability, structural governance and AI-specific security aspects. The implementation roadmap prioritised three critical risks:

- 1. AI system reliability and robustness**  
Developing verification and validation processes and comprehensive monitoring frameworks (e.g. through machine learning operations)
- 2. AI governance gaps**  
Establishing formal governance structures and defining roles and responsibilities
- 3. AI-specific security vulnerabilities**  
Documenting security controls and implementing targeted strategies to minimise vulnerabilities

This structured and risk-oriented approach enabled the AI management system to be rolled out in a targeted manner while using resources efficiently – without overwhelming the organisation across the board.

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

### Recommendations for similar organisations

The experience of ANYbotics shows several critical success factors for the implementation of ISO/IEC 42001:

- **Management support** is crucial. Management support is essential for allocating resources and overcoming internal hurdles during the governance transformation.
- **Building on existing structures** instead of starting from scratch. The established information security management and safety processes form a solid foundation. This shows how existing governance structures can be used and expanded – with time savings and minimal disruption to operational processes.
- **External expertise** is a key success factor. Support from specialist consultants in the gap ana-

## 03. Sandbox project with ANYbotics

---

ysis helps to avoid typical pitfalls and accelerate internal learning, especially in areas with little internal governance experience.

- **A comprehensive risk analysis** forms the basis for all further steps. This is the only way to focus resources on the most effective measures.
- **Seamless documentation** of all processes and decisions creates the traceability necessary for certification.
- **Quick wins** during the course of the project also help to maintain motivation over the long implementation period.

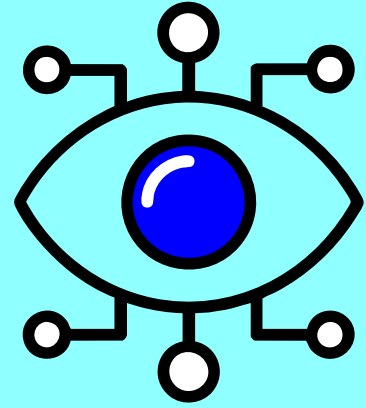
### Implementation challenges

Organisations should also avoid typical mistakes:

- **Implementation in all areas at the same time** overwhelms the teams and distracts from priority risks.
- **Not carrying out impact assessments** can lead to blind spots not being discovered until the audit.
- **Isolating existing governance structures** leads to unnecessary conflicting objectives and duplication.
- **Cultural change** is often underestimated – a lack of change management slows down acceptance.
- Delayed set-up of **monitoring systems** prevents early detection of implementation gaps, which can lead to significantly higher costs further down the line.

# 04.

## *Conclusion and outlook*



**Based on the legal analysis of the most important EU regulations and the practical experience gained from the use case, key fields of action emerge for companies. The following sections combine these findings in the form of overarching recommendations for regulation, risk management and innovation promotion.**

---

### **1. Systematic integration of regulatory requirements**

The increasing density of regulations in the field of AI and robotics calls for a systematic approach in order to consistently embed new requirements into existing development and management processes. The example of autonomous inspection robots shows that companies need to link technical innovations with regulatory requirements at an early stage – especially for safety-critical functions and for use in critical infrastructures. The aim is to establish a consistent governance framework that integrates new legal requirements such as the EU AI Act, the EU Machinery Regulation or the EU Cyber Resilience Act, as well as voluntary standards such as ISO/IEC 42001. This enables companies to identify regulatory developments at an early stage, understand dependencies and further develop existing structures efficiently, without having to set up separate sys-

tems for each new set of rules. Experiences from test environments such as the AI sandbox also demonstrate that interdisciplinary collaboration makes a decisive contribution to operationalising requirements in a practical way and anchoring them sustainably in corporate management.

### **2. Role of standards and management systems**

In addition to legal requirements, voluntary standards are becoming increasingly important – both for internal governance and for building trust externally. ISO/IEC 42001 is the first standard for a structured AI management system. For companies that use AI in safety-critical fields such as autonomous inspection, this standard can create a competitive advantage in the medium term, such as in tenders, international partnerships or industry-specific guidelines. The sandbox project with ANYbotics and Modulos shows that ISO/IEC 42001 offers valuable guidance, especially in connection with EU regulations such as the AI Act (e.g. in the areas of risk management and documentation obligations).

### **3. Combination of traditional and AI-specific requirements**

Future regulatory frameworks must consistently combine traditional safety requirements (e.g. under the EU Machinery Regulation) with the characteristics of dynamic, adaptive AI systems.

## 04. Conclusion and outlook

A risk-based approach forms the core of this approach: it takes into account physical hazards, as well as digital and algorithmic risks. Adaptive conformity assessments focus specifically on AI-related properties, such as adaptive algorithms, changing models or context-dependent decision logics. Depending on the risk level, differentiated testing and verification requirements will apply – from technical documentation for static systems to the validation of training data and models for learning systems to external audits for safety-critical, non-deterministic applications. In addition, continuous monitoring and update obligations ensure fulfilment of security and compliance requirements even after the product has been placed on the market.

### 4. Defining AI systems in complex robotics applications

A key issue in the risk assessment and regulation of complex robotic systems is whether the system as a whole or only individual AI components should be considered. While a system evaluation covers the interactions between different modules, a component-based evaluation can be useful when individual AI building blocks – such as for navigation or motion control – are reused in different products. For the risk analysis, it is also decisive whether the focus is on the application (e.g. failure to detect a defect) or on the operational safety of the robot itself (e.g. a physical malfunction). A clearly defined valuation model not only supports regulatory traceability, but also enables flexible reuse of certified modules in different contexts. Companies should therefore document at an early stage the level at which the assessment takes place and differentiate their risk management strategies accordingly. In this way, regulatory requirements can be met consistently and synergies in development and certification can be exploited at the same time.

### 5. AI test environments as learning spaces

Test environments for autonomous inspection robots create interdisciplinary learning spaces in which companies, research institutions and authorities can jointly test security, AI behaviour and regulatory requirements in practice. Regulatory experiment clauses or pilot articles allow temporary and limited exemptions from existing legal requirements in order to test innovative AI systems under realistic conditions. Official supervision remains key, supplemented by protective measures for safety and fundamental rights. These kinds of test environments thereby make a significant contribution to implementing regulatory requirements in a practical way and promoting innovation in a responsible manner.

*«Future-ready robotics emerges when technical progress and AI governance go hand in hand.»* Raphael von Thiessen, AI Sandbox Programme Manager, Canton of Zurich

# Glossary

---

## ***ATEX certification***

EU certification for equipment used in potentially explosive atmospheres. ATEX certification is required for operating autonomous robots such as ANYmal X in sensitive industrial environments.

## ***Digital twins***

Virtual images of physical systems that are continuously fed with real-time data. They are used for condition monitoring, simulation and decision support – particularly in autonomous inspection and predictive maintenance.

## ***EU Cyber Resilience Act***

EU Regulation to improve the cybersecurity of connected digital products and services. It defines design, development and maintenance requirements – with direct relevance for AI-based, network-enabled robotics systems.

## ***EU Data Act (Data Act)***

EU Regulation to promote fair access to and use of data. In particular, it governs access to and use of data generated by connected devices or services – with implications for AI-based inspection systems.

## ***EU AI Act (AI Act)***

EU Regulation governing artificial intelligence. It classifies AI systems by risk level (e.g. minimal, high or unacceptable) and defines specific requirements for development, transparency, safety and oversight.

## ***EU Machinery Directive***

Current EU Directive on the safety of machinery and its placing on the European internal market. It defines basic health and safety requirements for the design, construction and operation of machinery. It will be replaced in full by the new EU Machinery Regulation in 2027.

## ***EU Machinery Regulation***

Successor to the EU Machinery Directive. As a Regulation, it is directly applicable in all Member States and contains updated requirements for safety, digitalisation and the use of AI in machinery. Among other things, it sets out obligations for manufacturers and takes into account the interaction with the EU AI Act.

## ***General purpose AI***

AI systems that are not just developed for a single, specific purpose, but instead can be used in a variety of applications and contexts. General purpose AI is characterised by its broad functionality and can cover both general tasks (e.g. word processing, image recognition or speech interaction) and specialised applications in various industries.

## ***Internal production control***

A conformity assessment procedure in which the manufacturer declares under its sole responsibility that a product complies with the applicable legal requirements. In the context of the EU Machinery Regulation, this means companies are allowed to check and document the compliance of their machinery with the relevant health and safety requirements themselves.

## ***ISO/IEC 42001***

International standard for the management of AI systems. Its aim is to ensure that organisations use AI responsibly, securely and comprehensibly – including governance structures, risk management, transparency and stakeholder engagement. The standard is particularly relevant for companies that develop or operate AI systems in safety-critical areas.

# Glossary

---

## ***AI regulatory sandbox***

A test environment in which AI-based technologies – such as autonomous inspection robots – can be tested under real conditions. Companies, authorities and research institutions work together to clarify technical, legal and safety-relevant aspects at an early stage. Regulatory sandboxes enable risk-aware testing before broad market deployment.

## ***Conformity assessment***

Process for checking whether a product or system meets the regulatory requirements (e.g. under the EU AI Act or the EU Machinery Regulation). Depending on the risk class, this can be done through internal audits, external audits or notified bodies.

## ***LIDAR (light detection and ranging)***

An optical measuring method for precise distance measurement and ambient detection. LIDAR systems emit laser pulses and measure the time until the light is reflected from objects. Three-dimensional maps of the environment can be created from this data. In robotics, LIDAR is used in particular for navigation, obstacle detection and mapping (e.g. in the context of SLAM).

## ***Notified body***

An independent, officially appointed testing organisation that assesses EU conformity for certain products. Autonomous inspection robots with safety-relevant AI function (e.g. obstacle avoidance) must be switched on if self-certification is not permitted in accordance with the EU Machinery Regulation.

## ***Reinforcement learning***

A branch of machine learning in which an AI system learns to perform certain tasks optimally through targeted interaction with its environment. In the context of autonomous robots, reinforcement learning is used to control the locomotion: the robot learns how to move stably and efficiently over complex terrain – such as by climbing stairs or bypassing obstacles.

## ***SLAM (simultaneous localisation and mapping)***

A process from robotics and computer vision that allows a mobile system to orient itself in an unfamiliar environment (localisation) and create a map of this environment (mapping). SLAM is typically implemented using sensors such as LIDAR or cameras and is central to autonomous navigation without external reference systems such as GPS.

## ***Supervised learning***

A machine learning process in which a model learns from labelled training data to recognise certain patterns or make predictions. Autonomous robots use supervised learning to evaluate visual, thermal and acoustic inspection data – such as to detect display values, unusual noises or temperature deviations on machinery.

# Authors

---



**Stephanie Volz**  
Managing Director ITSL,  
University of Zurich



**Raphael von Thiessen**  
AI Sandbox Programme Manager,  
Canton of Zurich



**Sven Kohlmeier**  
Specialist Attorney for IT Law,  
Wicki Partners AG

## Case study from the Innovation Sandbox for AI

A case study was provided by ANYbotics with its autonomous inspection robot ANYmal. ANYbotics submitted a project proposal to the Sandbox in summer 2024. The content of this report was developed on the basis of this specific case study.

# Impressum

---

## **Publisher**

Standortförderung, Kanton Zürich  
Verein Metropolitanraum Zürich  
Innovation Zurich

## **Project conception and coordination**

Raphael von Thiessen  
Standortförderung Kanton Zürich  
8090 Zürich  
raphael.vonthiessen@vd.zh.ch

## **Concept in collaboration with**

Stephanie Volz  
Isabell Metzler  
Patrick Arnecke  
Markus Müller

## **Authors**

Raphael von Thiessen  
Stephanie Volz  
Sven Kohlmeier

## **Design**

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

## **Publication**

This report is published exclusively in digital format  
and is available in German and English.

## **Translation**

Supertext AG

## **Copyright**

All content of this publication, in particular texts and graphics, is protected by copyright. The copyright is held by the Office for Economic Development of the Canton of Zurich. The publication may be shared with proper attribution and may be quoted from, provided the source is fully cited.

## **Project-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