Physical AI and regulatory compliance in the EU

Georgia & Molly | September *2026*

A summary overview of the applicable AI, product safety, cybersecurity and data protection regulations for connected physical products with AI components

Background and purpose

This article summarises a legal review addressing regulatory compliance for products marketed under the term 'Physical AI' – physical products, such as robots, drones, industrial machinery and consumer electronics, which contain AI components and, in some cases, are connected to networks. The review is limited to EU law, with a particular focus on the AI Regulation, the Machinery Regulation, the Cyber Resilience Act and the GDPR.

1. What is Physical AI?

"Physical AI" is not a defined legal term in EU legislation, but rather an industry term for AI systems that are physically embodied and operate in the real world – robots, autonomous vehicles, drones and other physical products that use AI to perceive their surroundings and act within them. This differs from "digital AI", which produces text, images or recommendations in a digital environment without any physical impact.

As the term has no legal status of its own, the legal assessment must instead be based on the EU's AI Regulation (Regulation (EU) 2024/1689), which defines an 'AI system' in a technology-neutral manner: a machine-based system designed to operate with varying degrees of autonomy and which, based on the input it receives, can generate outputs such as predictions, content, recommendations or decisions that may affect physical or virtual environments. This definition therefore encompasses both digital AI and Physical AI as the same legal category.

In practice, Physical AI products are covered by several interrelated regulatory frameworks: the risk classification under the AI Regulation, the Machinery Regulation (for machines and robots), the Cyber Resilience Act (for connected products), the Product Liability Directive, and sector-specific legislation such as the Radio Equipment Directive, the EMC Directive and the Low Voltage Directive.

2.The AI Regulation: classification and risk assessment

The AI Regulation follows a risk-based model whereby a higher risk of harm triggers stricter requirements. Two separate pathways lead to a high-risk classification: firstly, Article 6(1), which applies to AI systems that are safety components in, or themselves constitute, products covered by the harmonisation legislation in Annex I; and Article 6(2), which applies to stand-alone AI systems listed in Annex III (for example, biometrics, recruitment and credit scoring), regardless of any connection to a physical product. Only the first route is directly relevant to Physical AI in the strict sense.

A ‘safety component’ is defined in Article 3(14) as a component of a product or an AI system that fulfils a safety function, or whose failure or malfunction endangers human health and safety or property. A component fulfils a safety function when its intended purpose is to prevent or reduce such risks. The Digital Omnibus on AI (Regulation (EU) 2026/1744) clarified that the mere fact that an AI system is integrated into a product covered by harmonised legislation does not in itself make it a safety component, and that AI systems used solely for user support, performance optimisation or convenience do not count as safety components – unless their failure or malfunction would jeopardise health and safety, in which case they are always considered safety components.

2.1 The role of machine learning and adaptivity in classification

Machine learning and adaptivity are not in themselves decisive for classification. Adaptivity (the ability to demonstrate adaptability after deployment) is, according to the definition of an AI system, a possible but not necessary characteristic – a static, pre-trained system can still be an AI system if it infers outcomes from input data. The classification as high-risk is instead determined by the safety function: a non-adaptive AI model controlling a safety-critical function may be a safety component, whilst a continuously learning but purely convenience-oriented function may be entirely exempt.

For the same reason, it is generally not sufficient to simply disable the learning function to avoid regulation. AI status does not require active learning, and the high-risk classification is determined by the safety function and the risk in the event of a malfunction, which normally remains unchanged regardless of whether the underlying model is static or learning.

2.2 Example: robot vacuum cleaner

A traditional robot vacuum cleaner that navigates using fixed, pre-programmed rules without inference from sensor data normally falls entirely outside the scope of the AI Regulation. An AI-component-based robot vacuum cleaner that uses computer vision or probability-based room mapping is likely to meet the definition of an AI system, but will only be classified as high-risk if the AI function has the intended purpose of preventing risk (for example, obstacle or stair detection to avoid personal injury), or if its malfunction would jeopardise safety – regardless of whether the function merely optimises cleaning patterns.

3. Third-party conformity assessment

High-risk classification under Article 6(1) requires that two conditions be met simultaneously: the AI system must be a safety component in a product covered by the harmonised legislation listed in Annex I, and the product must already require third-party conformity assessment under the underlying product legislation. The requirement for third-party assessment therefore always stems from the product legislation itself – not from the AI Regulation.

The Digital Omnibus on AI clarified that classification as a high-risk AI system under Article 6(1) does not in itself necessitate third-party assessment: if the underlying product legislation permits the manufacturer’s own declaration of conformity, this continues to apply even where a high-risk AI system is incorporated.

For machinery (including robots), the matter is governed by the Machinery Regulation (Regulation (EU) 2023/1230). Machinery listed in Annex I, Part A – the most serious categories – always requires a procedure involving a notified body. Machinery listed in Annex I, Part B, may be assessed through the manufacturer's own declaration, provided that the product is designed in accordance with the applicable harmonised standards; otherwise, a third-party procedure is required. Machinery not listed in Annex I is always subject to internal production control without third-party involvement. Under the Digital Omnibus on AI, the Machinery Regulation was moved to Section B of Annex I to the AI Regulation in order to coordinate AI-related safety requirements directly within the machinery assessment, with application by 2 August 2028 at the latest.

A specific exception applies if third-party assessment is required solely for reasons unrelated to health and safety, such as radio spectrum or electromagnetic risks – this does not count as fulfilment of the third-party assessment requirement in Article 6(1).

4. CE marking and market authorisation

In practice, CE marking is required for almost all Physical AI product categories, but this stems primarily from the underlying sector-specific legislation rather than from the AI element as such.

Robots and industrial machinery that constitute 'machinery' within the meaning of the Machinery Regulation must always bear the CE marking before being placed on the market or put into service, regardless of their AI content. Drones (unmanned aircraft systems) are covered by Regulation (EU) 2019/945, which requires an EU declaration of conformity and CE marking according to weight-based risk classes (C0–C6), with an associated class identification label. Consumer electronics are normally covered by the Radio Equipment Directive (if they have a radio function), the EMC Directive and/or the Low Voltage Directive, all of which require CE marking.

The AI Regulation becomes relevant to the content of the CE assessment – rather than to the marking requirement itself – when the product's AI function qualifies as a safety component: in which case, the substantive requirements of the AI Regulation (risk management, documentation, robustness, human oversight) must be incorporated into the existing assessment process, regardless of whether this is carried out through self-declaration or by a notified body.

4.1 Substantial modification following CE marking by a third-party supplier

Where a product has already been CE-marked by a subcontractor but is subsequently modified (for example, through software changes, the addition of new sensors, or the addition of a connectivity unit), it must be assessed whether the modification constitutes a 'substantial change' under Article 3(16) of the Machinery Regulation. The definition has four cumulative criteria: a modification, by physical or digital means, occurring after the product has been placed on the market, which was not foreseen or planned by the original manufacturer, and which creates a new risk or increases an existing risk in a way that requires the addition of protective devices necessitating a change to the safety control system, or further stability or strength measures.

Under Article 18, the party carrying out a substantial modification is to be regarded as the manufacturer within the meaning of the Regulation, with all the manufacturer's obligations under Article 10 – new technical documentation, a new assessment procedure, a new EU declaration of conformity and new CE marking under their own name. In a typical scenario involving software modification, new sensors and an already CE-marked connectivity unit, the addition of safety-related sensors is the modification most likely to constitute a substantial change, whilst a standalone connectivity component with no link to safety functions is less likely to do so under the Machinery Regulation – even though it may trigger separate obligations under the Cyber Resilience Act. The assessment should be carried out both for each individual change and for their combined effect.

5. The Cyber Resilience Act and connected products

The Cyber Resilience Act (Regulation (EU) 2024/2847) applies to 'products with digital elements' whose intended purpose or reasonably foreseeable use involves a direct or indirect logical or physical data connection to a device or network. A connected robot or other physical AI product with a connectivity function normally meets this criterion and is therefore covered by the Regulation, unless a sectoral exemption applies (medical devices, vehicle type-approval, certified civil aviation, marine equipment, or products for national security and defence).

Products whose core function corresponds to a category in Annex III are classified as 'critical products with digital elements' and are subject to stricter assessment procedures – this applies to functions that are critical to the cybersecurity of other products or that could disrupt, control or harm a large number of other products or the health and safety of users. However, the mere fact that such a component is integrated into another product does not in itself make the entire product a 'critical product'. The strictest categories, 'critical products' as defined in Annex IV, require high-assurance certification and are reserved for products of central importance to the cybersecurity of entities of critical importance to society.

The Cyber Resilience Act has its own definition of 'substantial change', distinct from that in the Machinery Regulation – a change made after placing on the market that affects compliance with the essential cybersecurity requirements or alters the intended purpose. A modification (for example, the addition of a connectivity unit) may therefore constitute a substantial change under the Cyber Resilience Act even if it does not do so under the Machinery Regulation, as the assessment there relates to cybersecurity risk rather than physical safety.

6. Data protection requirements under the GDPR

Connected physical AI products with sensors (cameras, microphones, location and motion data) often collect personal data and thus fall within the scope of the GDPR. In the absence of robot-specific guidance, the European Data Protection Board's guidance on connected vehicles provides the most relevant framework: particular attention should be paid to location data, biometric data and data that may reveal crimes or offences, as these categories are particularly sensitive in terms of privacy.

For each purpose of processing, a legal basis under Article 6 must be established. Data protection by design and by default under Article 25 require the data controller, as early as the product design phase, to take into account the nature, scope, context and purposes of the processing, as well as the risks to the rights of data subjects, and to ensure that protective measures are kept up to date in line with technological developments ('state of the art'). Practical measures recommended for connected products include data minimisation, privacy-friendly default settings, and – where possible – local data processing within the product rather than transfer to external systems, which reduces both privacy and cybersecurity risks.

A data protection impact assessment (DPIA) under Article 35 is required where the processing is likely to result in a high risk to the rights and freedoms of data subjects – which is typically the case for products that combine AI-driven sensor processing with a physical presence in home or work environments. Failure to carry out a DPIA where required may result in administrative fines.

7. Prioritised compliance steps

Based on the review, the process of introducing a connected robot with an AI component to the EU/EEA market can be structured into four phases.

7.1 Phase 1 – Basic classification

Classify the status of the AI component in accordance with the AI Regulation (AI system, safety component); classify the product in accordance with Annex I of the Machinery Regulation; classify the product in accordance with the risk categories set out in the Cyber Resilience Act; and map all processing of personal data along with the associated legal basis.

7.2 Phase 2 – Design and documentation

Carry out an integrated risk and impact assessment that comprehensively covers physical security, AI-specific risks, cybersecurity and data protection (DPIA), implement built-in data protection and secure default settings, and draw up technical documentation covering all applicable regulations.

7.3 Phase 3 – Conformity Assessment

Carry out the relevant assessment procedures under the Machinery Regulation and the Cyber Resilience Act, draw up the EU Declaration of Conformity and affix the CE marking, and register the product in the relevant EU databases if it is classified as high-risk under the AI Regulation.

7.4 Phase 4 – Market launch and ongoing compliance

Publish a privacy policy and user information prior to launch; establish processes for vulnerability management and incident reporting in accordance with the Cyber Resilience Act, as well as for personal data breaches in accordance with the GDPR; and establish a process for assessing future changes against the concept of a 'substantial change' in both the Machinery Regulation and the Cyber Resilience Act before each update is rolled out.

An important point to note concerns the timetable: the high-risk rules of the AI Regulation for product-embedded AI systems, as set out in Article 6(1) and Annex I, will apply, following the Digital Omnibus amendment, from 2 August 2028, whilst fundamental obligations (such as the prohibition of certain AI methods and requirements for AI competence) already apply. The timetables set out in the Machinery Regulation and the Cyber Resilience Act run independently of this.

SUMMARY CONCLUSION

Compliance for Physical AI products requires a coordinated assessment across multiple regulatory frameworks, each of which has different triggering criteria and dates of application. The AI Regulation adds substantive requirements on top of existing product safety rules rather than replacing them, which means that the key task for a manufacturer is to correctly identify which combination of the Machinery Regulation, the Cyber Resilience Act, sector-specific product legislation and the GDPR that applies to the specific product, and to establish an integrated – rather than fragmented – process for risk and impact assessment, technical documentation and conformity assessment.

ABOUT THIS ARTICLE

This article summarises a legal dialogue focused on EU law (the AI Regulation 2024/1689, the Digital Omnibus on AI 2026/1744, the Machinery Regulation 2023/1230, the Cyber Resilience Act 2024/2847, the Product Liability Directive 2024/2853, as well as the GDPR and associated guidance from the European Data Protection Board). It does not cover national implementing legislation, guidance from the AI Agency or national supervisory authorities, or regulatory frameworks outside the EU/EEA. The conclusions are based on a general product description and should be verified against the specific product's technical specifications before being used as the basis for market launch.