

Cheat Sheet: Compliance for Connected Robot with AI

This checklist provides a step-by-step plan for meeting EU/EEA regulatory requirements for a connected robot with AI components. It integrates the AI Act, the Machinery Regulation, the Cyber Resilience Act (CRA), and the GDPR.

PHASE 1: Mapping & Classification (Initial Phase)

To be done early in the project to understand which regulatory frameworks apply.

The AI Act

- ☐ **Is it an AI system?** Assess whether the system infers outcomes from input data to influence the physical environment.
- ☐ **Is it a safety component?** Determine if the AI's intended purpose is to prevent/mitigate risks to health/safety/property, or if its failure endangers this. (*NOTE: Purely performance- or convenience-enhancing AI functions do not count as safety components*).

The Machinery Regulation

- ☐ **Classify the machinery:** Does the robot belong to Annex I Part A (requires third-party assessment), Part B (self-declaration via harmonised standards possible), or is it unlisted?

The Cyber Resilience Act (CRA)

- ☐ **Classify the product:** As a connected device, it is a "product with digital elements". Does it fall under a *default, important* (Annex III), or *critical* (Annex IV) product category? Do any sectoral exemptions apply?

Data Protection (GDPR)

- ☐ **Map data flows:** What personal data is collected? (e.g., camera feeds, audio, location data, biometrics).
- ☐ **Legal basis:** Establish a legal basis (consent, contract, legitimate interest) for *each* processing purpose (e.g., operation, profiling, troubleshooting).

Other Directives

- ☐ Identify if the Radio Equipment Directive (RED), EMC Directive, or Low Voltage Directive (LVD) are applicable.

PHASE 2: Design & Documentation

Integrate the requirements into the product's architecture.

- ☐ **Integrated Risk Assessment:** Conduct a comprehensive risk analysis covering:
 - Physical safety (Machinery Regulation)

- AI-specific risks (AI Act, if high-risk)
 - Cybersecurity (CRA)
- [] **DPIA (GDPR):** Conduct a Data Protection Impact Assessment. (*Assume this is required for this type of product combining AI, sensors, and physical presence*).
- [] **Data Protection by Design and by Default:** Design for data minimisation, privacy-friendly default settings, and (preferably) local data processing on the robot rather than in the cloud.
- [] **Joint Security Design:** Coordinate the cybersecurity measures (CRA) with the technical security requirements for data protection (GDPR Art. 32).
- [] **Technical Documentation:** Begin compiling the comprehensive technical documentation proving the robot complies with *all* applicable regulations (preparation for CE marking).

PHASE 3: Conformity Assessment & Approval (Pre-launch)

The critical path to placing the product on the market.

- [] **Choose assessment procedure:** Is internal production control (self-declaration) sufficient, or is a Notified Body (third-party assessment) required? This is primarily dictated by the Machinery Regulation and the CRA.
- [] **Conduct the assessment:** Carry out the chosen conformity assessment based on the technical documentation.
- [] **EU Declaration of Conformity & CE Marking:** Draw up a single EU Declaration of Conformity (covering Machinery, CRA, and potentially RED) and affix the CE marking.
- [] **Transparency & Registration:**
 - Publish the privacy policy and user information.
 - *If high-risk AI:* Register the product in the relevant EU databases (AI Act).

PHASE 4: Post-Market & Continuous Compliance

Activities ongoing throughout the product's lifecycle.

- [] **Incident & Vulnerability Management:** Establish processes to detect and report cybersecurity vulnerabilities (CRA) and personal data breaches (GDPR).
- [] **Handling Substantial Modifications:** Create a process to evaluate all future software and hardware updates:
 - *Does the AI function change?*
 - *Is physical safety impacted (Machinery Regulation)?*
 - *Is cybersecurity impacted (CRA)?*
 - **NOTE:** If an update constitutes a "substantial modification", a new conformity assessment must be carried out.

Important Timelines

- **The AI Act (High-Risk):** The rules for product-embedded AI systems apply from **2 August 2028** (however, fundamental prohibitions and AI literacy requirements apply sooner).
- **Machinery Regulation & CRA:** These have their own independent timelines that must be adhered to regardless of the AI Act's dates.