CEO Briefing: The New Era of EU Hardware Compliance (2026)

If you are leading a hardware company building anything from industrial humanoids to consumer electronics, your regulatory roadmap has fundamentally changed. As of May 2026, the EU has moved beyond simple physical safety to a complex landscape of software integrity, data ethics, and circularity.

The critical takeaway for your executive team: **Self-assessment is no longer a guaranteed option**. For products in stricter risk categories, you must now factor in the time and cost of a "Notified Body" (a third-party auditor) to certify your product before it can be legally sold.

1. Machine Regulation (2023/1230)

This regulation addresses the intersection of mechanical hardware, AI, and cybersecurity.

- **Cybersäkerhet for Safety:** For the first time, cybersecurity is a core safety requirement.
- **Integrity of Safety Functions:** If a machine's safety functions, such as an emergency stop, can be compromised by a remote hack or software corruption, it fails compliance.
- **Autonomous & Self-Evolving AI:** The regulation introduces specific safety requirements for machines with "self-evolving" behavior to ensure they remain within an intended "safety zone".
- **Mobility Safety:** There are stricter rules for AGVs and AMRs to ensure safe interaction with human workers.
- **Substantial Modification:** Modifying an old machine in a way that creates new risks makes you legally the "manufacturer," requiring a full re-CE marking of the unit.
- **Digital Documentation:** Manufacturers are now permitted to provide digital manuals rather than printed copies. EU.

2. AI Act (2024/1689)

This act uses a risk-based approach: the higher the risk to human rights and safety, the stricter the rules.

- **High-Risk Classification:** AI used for safety mechanisms in robots or forklifts is considered high-risk and requires third-party certification.
- **Prohibited Practices:** Applications involving social scoring or emotion recognition are banned.
- **Transparency for Limited Risk:** Systems like chatbots and deepfakes must be clearly disclosed to users.
- **May 2026 Update:** As part of the **Digital Omnibus** package, the AI Act has been slightly simplified and some requirements have been postponed.

3. Cyber Resilience Act (CRA) (2024/2847)

TheThis serves as a mandatory "CE Mark for Cybersecurity" for all connected devices and software.

- **Risk Categories:** While 90% of products fall into the "Default" category (e.g., smart toys), "Critical" products like industrial control systems require third-party certification.
- **Prevention of Attacks:** Every connected device must now be certified to prove it cannot be easily hacked.

4. Battery Regulation (2023/1542)

This is the first EU legislation to take a full life-cycle approach to a product.

- **Digital Product Passport:** Batteries are among the first products (alongside textiles and wood) required to have a digital passport.
- **Sustainability & Carbon Footprint:** You must declare the carbon footprint of your batteries, which will eventually be sorted into performance classes.
- **Circular Design:** Products must be designed for easy battery removability and replaceability.
- **National Registration:** You must register in the national producer registers of every Member State where you sell.

5. Packaging and Packaging Waste (PPWR) (2025/40)

Though it may seem less technical than the AI Act, the process-side requirements for packaging are extensive.

- **Declaration of Conformity (DoC):** Every unique packaging type requires a technical file and a signed legal document proving it meets standards for substances and minimization.
- **Packaging Minimization:** Manufacturers must prove that their packaging is the "minimum necessary" for safety and functionality.
- **National Registration:** You must register in the national producer registers of every Member State where you sell (same as for batteries).

Your immediate action items:

- **Identify your risk tier:** Determine if your product allows for self-certification or if you need to book a Notified Body for an external audit.
- **Audit your software supply chain:** The CRA and Machine Regulation now make you legally responsible for the "safety" and cybersecurity of your code.
- **Review packaging and product design:** Ensure your R&D team is designing for “safety first,” "removability," and "minimization" now to avoid costly redesigns later.
- **Processes for passports & reporting:** Run trials for both digital passports and EPR reporting to ensure that you have the required data and the systems to submit it.