EU CYBER RESILIENCE ACT: TRENDS, CHALLENGES, AND OPPORTUNITIES WHITE PAPER

Dr Anna Aseeva
(Policy & Sustainability Expert, Digital For Planet)

PhD Cand. Karolina Gyurovszka
(Policy Analyst and Consultant, Martel Innovate)

martel-innovate.com | digital4planet.org

TABLE OF CONTENT

+ EXECUTIVE SUMMARY

- The Cyber Resilience Act (Regulation (EU) 2024/2847) sets binding cybersecurity standards for every product with digital elements sold on the EU market—and it holds **the organisations behind those products fully accountable**
- The CRA is the first EU-wide 'rulebook' that ensures **any product with a digital pulse** (from smart toys and home cameras to business accounting software) is built **with security in mind from day one**
- Just like a safety rating for a car, it mandates that devices are **'secure by design'** and receive regular updates to keep hackers out throughout their lifespan
- **The first hard deadline hits September 11, 2026**
- CRA extends to all manufacturers wishing to market products in the EU, **regardless of their physical location**
- If you sell digital products in the EU, the CRA applies to you—**even from Switzerland**
- **Non-compliance** can mean **fines**, **blocked market access**, or reputational **damage**: those who do not comply are looking at fines of up to €15 million or 2.5% of global annual turnover, whichever is higher.

+ IS CRA A NEW GDPR?

The General Data Protection Regulation (GDPR)[1] is widely regarded as one of the world's most robust data protection frameworks. It governs how individuals—and increasingly, algorithms—access, process, and use personal data, establishing clear boundaries for organisations and businesses. GDPR has impacted privacy laws in over 100 countries worldwide.[2] In doing so, it has contributed not only to stronger data protection but also to **shaping a more human-centric European and global digital ecosystem**.

Despite several recent headwinds, the EU continues to leverage its massive single market to project its regulatory values extraterritorially. The Cyber Resilience Act (CRA),[3] just as the Artificial Intelligence Act (AI Act),[4] carries sweeping extraterritorial mandates—and can thus be seen **a 'new GDPR'**.[5] The AI Act applies to any entity placing AI systems on the EU market, regardless of where the provider is headquartered. Similarly, the CRA establishes legally binding, lifecycle cybersecurity requirements for any 'product with digital elements' (PDE) made available on the EU/EEA market.[6]

The strategic objective of these laws is to construct **a 'third way'** for the innovation system—one that differs from both the dominance of US corporate-state power coalitions over innovation infrastructure and Chinese digital authoritarianism,[7] while compelling foreign manufacturers to align their technical designs with European public policy objectives.[8]

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). OJ L 119.

[2] Anna Aseeva, 'Liable and Sustainable by Design: A Toolbox for a Regulatory Compliant and Sustainable Tech ' (2024) 16(1) *Sustainability* art 228 pp 27. DOI: https://doi.org/10.3390/su16010228.

[3] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). OJ L 327.

[4] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). OJ L 1689.

[5] Hung-Yi Chen, 'AI Governance and Regulation 2026: A Complete Guide to Global Frameworks', https://www.hungyichen.com/en/insights/ai-governance-regulatory-landscape-2026.

[6] EU Cyber Resilience Act's Impact on Swiss Companies - Homburger, https://www.homburger.ch/en/insights/eu-cyber-resilience-acts-impact-on-swiss-companies.

[7] Hung-Yi Chen, op.cit, note 5.

[8] A. Bradford, *Digital Empires: The Global Battle to Regulate Technology*, Oxford University Press, 2023.

+ THE CONTEXT: MARKET POWER, INFRASTRUCTURAL CONTROL, AND EMBEDDED REGULATORY LOGICS

The intersection of market power and infrastructural control has fundamentally redefined the nature of technology governance.[9] To wit, as the digital economy has matured, a small cohort of **dominant platform operators** has captured critical bottlenecks in the physical and logical layers of the internet, including operating systems, cloud computing infrastructure, application programming interfaces (APIs), and app marketplaces.[10] This architectural centralisation grants these firms immense '**infrastructural power**'.[11] By controlling the software environments in which third-party developers operate, dominant platforms act as **private de facto regulators**, establishing **code-based rules** that govern transactional access, data collection, and software distribution.[12]

Namely, rather than relying on descriptive, paper-based compliance procedures, modern regulatory regimes seek to integrate **compliance requirements** and real-time supervisory access **directly into the software protocols** that facilitate transactions.[13] When platform operators wield this infrastructural power, they often construct vertical, closed ecosystems designed to protect their own commercial interests under the rhetorical banner of consumer security and privacy.[14]

The **European rights-driven model** seeks to counter this concentration of private power by **legally co-opting technical infrastructure**. By mandating principles such as *privacy by design* under the GDPR and *security by design* under the CRA, European regulators legally compel dominant platform operators and downstream manufacturers to realign their technical default settings with publicly-defined binding rules. In this manner, the EU attempts to transform the technology stack from a tool of **private corporate extraction** into a mechanism for public law enforcement and rights preservation. It also appears to be a way to assert **European digital sovereignty**—and the CRA, alongside the GDPR, is one of its core pillars.

[9] Id.
[10] Against Platform Regulation - OII Blogs, https://blogs.oii.ox.ac.uk/ipp-conference/sites/ipp/files/documents/OConnor-Schruers%2520-%2520Against%2520Platform%2520Regulation.pdf.
[11] Id.
[12] K. Pistor, 'Rule by Data: The End of Markets?', 83(2) *Law & Contemp. Probs*. 101 (2020). Available at: https://scholarship.law.columbia.edu/faculty_scholarship/2852 .
[13] D.A. Zetzsche, D.W. Arner, R.P. Buckley, 'Decentralized Finance', 6(2) *Journal of Financial Regulation*, 172 (2020). DOI: https://doi.org/10.1093/jfr/fjaa010.
[14] OII Blogs, op.cit., note 10.

+ MEET THE CYBER RESILIENCE ACT: MANDATES, TIMELINES, AND BOUNDARY TRIGGERS

The CRA is a sweeping, horizontal legislative instrument designed to integrate cybersecurity directly into the EU's product safety framework. The CRA establishes uniform cybersecurity requirements for all **products with digital elements** (PDEs)—defined as any software or hardware product intended or foreseeable to operate with logical or physical data connectivity to other devices or networks. By utilising a horizontal approach, the CRA covers a vast, heterogeneous array of technologies, including smart home appliances, browsers, operating systems, drones, and industrial control systems, while **exempting** only those sectors governed by equivalent, mature **vertical security rules**, such as **medical devices, motor vehicles,** and **civil aviation**.[15]

A core challenge of the CRA is its **extraterritorial authority**.[16] Because the regulation governs any product placed on the EU market, manufacturers and distributors domiciled outside the EU/EEA must comply to preserve market access.[17] This is of critical importance to Swiss industries, including Swiss SMEs in the IoT, precision machinery, and smart-manufacturing sectors, for whom the EU/EEA serves as the primary export market.[18] Moving forward, these non-EU exporters must absorb the technical and administrative costs of CRA compliance, reinforcing the rights-driven global influence of the EU.

The regulation pivots on **whether a product is placed on the market** in the course of a **commercial activity**.[19] To prevent choking open-source software development, the CRA defines **Free and Open-Source Software (FOSS)** as source code that is openly shared under a licence granting everyone the cumulative right to access, use, modify, and redistribute it.[20] However, FOSS is not exempt from the CRA if its distribution involves a commercial activity.[21] To clarify this distinction, the European Commission's draft guidelines under Article 26 establish a case-by-case evaluation framework that we detailed in a table in the Annex. Below is a summary of the types of activities and corresponding compliance burden:

[15] EU Cyber Resilience Act's Impact on Swiss Companies - Homburger, https://www.homburger.ch/en/insights/eu-cyber-resilience-acts-impact-on-swiss-companies; the EU Cyber Resilience Act – New Market Entry Barriers for Swiss IoT Products, https://www.mme.ch/en/magazine/articles/the-eu-cyber-resilience-act-new-market-entry-barriers-for-swiss-iot-products.

[16] A. Bradford, op.cit., note 8.

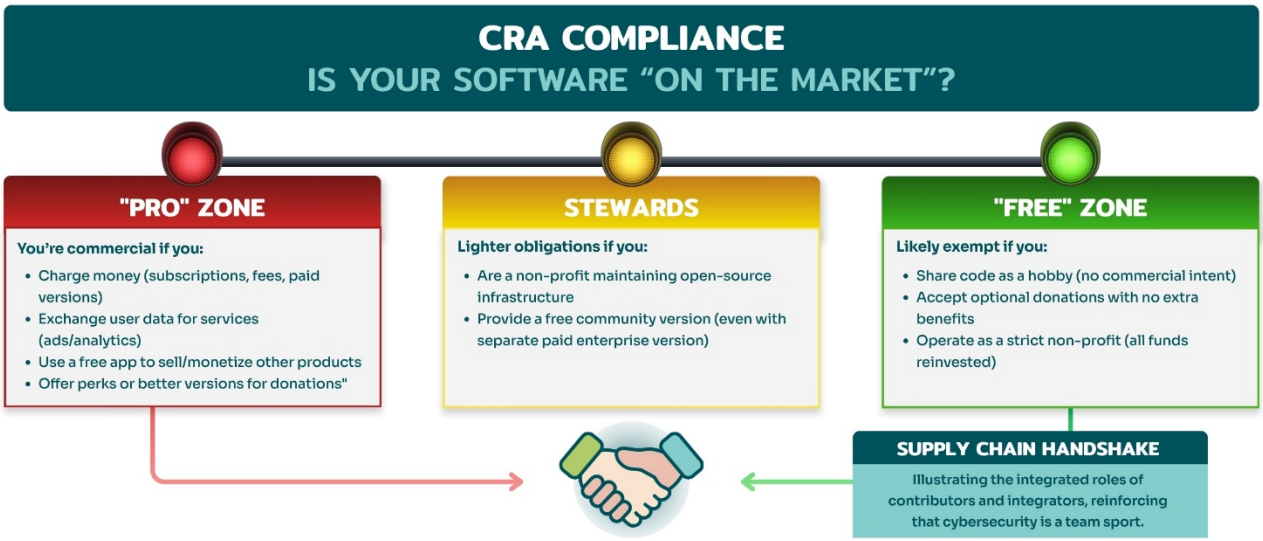
[17] CRA Articles 2-3.

[18] Idem. See also note 15.

[19] CRA Article 13(2).

[20] CRA Article 24.

[21] CRA Articles 24 and 26.



The implementation timeline for the regulation is highly compressed, requiring **immediate strategic planning by all covered economic operators**:

- **Entry into Force:** the CRA formally entered into force on December 10, 2024, following its publication in the Official Journal of the European Union.
- **Notification of Conformity Assessment Bodies (CABs):** by **June 11, 2026**, EU Member States must designate and notify the national CABs. This deadline establishes the essential third-party auditing infrastructure required to evaluate high-risk products.
- **The Article 14 Reporting Deadline:** on **September 11, 2026**, the first hard reporting obligations become legally binding.[16] Manufacturers are required to report any actively exploited vulnerabilities and severe security incidents via the European Union Agency for Cybersecurity (ENISA) single reporting platform within **24 hours** of becoming aware of them (early warning notification), followed by a detailed technical breakdown within **72 hours**.
- **Full Application:** on **December 11, 2027**, the CRA becomes fully applicable, meaning that no non-compliant PDE may legally be placed on the EU/EEA market.
- **Penalties for Non-Compliance:** Violations carry administrative fines of up to **€15 million or 2.5% of total worldwide annual turnover** for the preceding financial year, whichever is higher, alongside market restrictions, compulsory product withdrawals, and recalls.

+ DIFFERENT COMPLIANCE SCHEMES: SMEs/STARTUPS VS. OPEN-SOURCE STEWARDS

A critical strategic conflict exists regarding the structural capacity of different market actors to absorb the compliance demands of the CRA.

To analyse this, it is necessary to compare the legal obligations, operational costs, and systemic risks faced by commercial SMEs (acting as manufacturers) with those of Open-Source software stewards. While the CRA seeks to protect the software supply chain by holding manufacturers fully accountable, the operational realities of the two roles are fundamentally asymmetrical:

Comparative Dimension	Small & Medium Enterprises (SMEs) (as Manufacturers)	Open-Source Software Stewards (Article 24)
Legal Definition	Any natural or legal person who develops or manufactures a product with digital elements and markets it under its own name or brand.	A legal person, other than a manufacturer, systematically providing sustained support for the development of FOSS intended for commercial use.
CE Marking Conformity	**Mandatory**. Must perform conformity assessments, compile technical files, draw up declarations of conformity, and affix the CE mark.	**Prohibited**. Stewards are explicitly prohibited from affixing the CE marking to the open-source products they support.

Vulnerability Reporting	Full Article 14 compliance: Mandatory 24-hour early warning and 72-hour detailed notification of active exploits to ENISA.	Article 14 reporting obligations apply *only* to the extent that the steward is directly involved in the product's development.
Supply Chain Due Diligence	**High Burden**. Must exercise due diligence when integrating third-party components, including free and open-source software.	**Indirect Burden**. Must actively promote secure development practices and vulnerability documentation within the community.
Upstream Vulnerability Action	Must notify the upstream maintainer of any vulnerability found in integrated components and take steps to remediate it.	Must implement a policy covering how vulnerabilities are documented, addressed, and shared with the open-source community.
Document Retention	**Must maintain** all technical files and risk assessments for at least 10 years or the entirety of the support period (whichever is longer).	**No mandatory** 10-year technical file retention requirement; obligations are limited to documented cybersecurity policies.
Primary Risk Profile	Severe **vulnerability to financial penalties**, product recalls, market bans, and prohibitive operational overhead.	**Reputational risk** within the developer community and legal ambiguity regarding the boundary of 'sustained support'.

This comparative analysis demonstrates that the **compliance burden imposed on an SME** acting as a **manufacturer** is extraordinarily **heavy**. The requirement to perform continuous, documented cybersecurity risk assessments, establish a 24-hour automated alerting pipeline, and maintain ten years of technical documentation **requires highly skilled security personnel and sophisticated, automated compliance workflows**. For a typical SME or hardware-software startup, these mandates necessitate creating entirely new operational roles, which introduces significant, often non-viable overhead costs.

The cost of establishing a fully compliant software lifecycle process in line with European standards is likely to exceed the operational budget of a micro-enterprise or early-stage startup.

Faced with this structural asymmetry, SMEs are highly likely to engage in **regulatory *bricolage*** as a desperate survival mechanism.[22] Rather than investing in robust, certified security-by-design workflows, many small enterprises might resort to **'Frankenstein' compliance architectures** — using cheap, automated consumer-grade tools, or relying on non-specialist networks (such as interns or generalist developers) to sign off on technical documentation and risk assessments.[23] This improvised approach may satisfy the superficial, bureaucratic requirements of market surveillance authorities, but it fails to address the underlying physical security vulnerabilities of the products, **creating a dangerous gap between legal compliance and actual cyber resilience**.

Conversely, Open-Source stewards are governed by CRA Article 24, which imposes **a lighter, process-oriented burden**. Stewards must establish a documented cybersecurity policy that actively fosters secure development and coordinates vulnerability disclosures across their supported projects. However, the third-order implication of this dual-track structure is a major bottleneck in the software supply chain. **Because contributors are exempt and stewards cannot affix the CE mark, the *legal liability* for securing open-source components is *pushed entirely onto downstream commercial integrators*.**

This dynamic is poised to reshape the digital economy. Large platform operators, leveraging their massive capital, will easily establish automated screening pipelines to ingest, verify, and secure open-source components.[24] In contrast, resource-scarce startups and SMEs may find the cost of exercising due diligence on uncertified open-source libraries completely prohibitive. This could force SMEs to abandon the use of flexible, community-driven open-source software, driving them toward proprietary, expensive, pre-certified software suites provided by dominant technology incumbents.[25] Thus, the rights-driven regulatory logic of the CRA, when filtered through the reality of market asymmetries, also carries a risk of inadvertently reinforcing the structural power of dominant, well-capitalised digital empires.[26]

[22] N. Joulal & A. Messaoudi, 'Entrepreneurial Bricolage in the Face of Institutional Voids: The Case of Moroccan Startups', 13(2) *Sch J Econ Bus Manag*, 32(2026). DOI: https://doi.org/10.36347/sjebm.2026.v13i02.001.
[23] Id.
[24] Oll Blogs, op.cit., note 10.
[25] Id.
[26] A. Bradford, op.cit., note 8.

+ STRATEGIC RECOMMENDATIONS AND CONCLUSIONS

The convergence of global regulatory competition, extraterritoriality, and the operational rigidities of the CRA requires all covered operators to **fundamentally reorient their operational strategies**. To successfully navigate this emerging landscape, several key measures must be taken:

1) For SMEs: Transition from Paper-Based Compliance to Automated 'Embedded Regulation'

SMEs and small software developers must move away from retrospective, manual compliance audits, which are highly vulnerable to operational failure under the strict 24-hour reporting timelines of Article 14. Instead, organisations must implement the principles of 'embedded regulation' by integrating automated compliance and monitoring tools directly into their software development pipelines.

2) For Larger Organisations: Audit your Supply Chain

Organisations are legally responsible under the CRA for the vulnerabilities of their suppliers and sub-contractors across their entire supply chain. The EU-based firms should audit sub-processors now and prioritise those who can continuously prove a 'Compliant EU Supply Chain'. Crucially, when auditing smaller partners, they should utilise the simplified technical documentation forms (CRA Article 31; the Commission Guidelines on it). These concise templates enable SMEs in their value chain to prove compliance without the exhaustive overhead required of large operators. This directly bolsters strategic autonomy by ensuring local, small-scale innovators remain viable in the digital supply chain rather than being forced out by compliance costs.

Swiss organisations providing any products covered by the CRA to the EU market must comply with the CRA. Their EU clients are legally required to audit them, and failing to demonstrate a 'Compliant Supply Chain' may result in being excluded from EU procurement contracts. Crucially, for Swiss SMEs, a concrete survival strategy is to proactively utilise the forthcoming simplified technical documentation forms (CRA Article 31). These templates will allow them to comply without the massive administrative overhead, ensuring they remain competitively embedded in the EU digital supply chain without being priced out by bureaucracy.

3) For OS Developers & Operators: Establish Clear Legal Boundaries for Open-Source Integration

To meet the CRA's supply chain due diligence requirements, commercial integrators must draft and implement precise, automated procurement policies. When integrating free and open-source software, developers must distinguish clearly between FOSS projects supported by formal, well-capitalised Open-Source Stewards and those maintained by independent, voluntary contributors. Whenever possible, commercial integrators should prioritise components backed by established stewards who actively maintain documented cybersecurity policies under Article 24, as this significantly reduces the downstream manufacturer's risk assessment and due diligence burden.

4) Three Take-home Messages

1. Security is the new 'Safety Seal' for digital products

CRA mandates 'Secure by Design' as a market baseline:

- Establishes the first horizontal legal framework for any product with a digital pulse.
- Ensures cybersecurity is integrated from day one, not treated as an afterthought.
- Requires regular updates throughout a product's entire lifespan to keep hackers out.

2. Compliance is your passport to the EU market

CRA extends responsibility far beyond EU borders:

- Applies to any organisation selling digital products in the EU, including those in Switzerland.
- Early compliance provides a competitive advantage and prevents market access blocks.
- Rebalances responsibility by placing the duty of care squarely on the manufacturer.

3. Cybersecurity is a 'Team Sport' and a collective responsibility

CRA enables resilient organisational culture, not just a legal checklist. **It helps answer:**

- Is our product's lifecycle documented for sustainability and safety?
- Have we secured our supply chain and open-source integrations?
- Are entity's all roles—from Devs to CEOs—aligned on risk and incident response?

+ ANNEX - CASE-BY-CASE EVALUATION FRAMEWORK

Regulatory Status under the CRA	Commercial Activity Scenarios & Triggers	Impact & Compliance Level
Fully In Scope (Placed on the Market)	• Charging a direct purchase price or subscription fee for the software. • Bundling paid commercial support services with the software. • Gating access behind payment or donation tiers that grant contractual benefits. • Distributing a free app that monetizes users via in-app purchases or targeted advertising. • Making substantial modifications to FOSS as part of paid support or integration services.	**Full Manufacturer Obligations**: Must carry out conformity assessments, affix the CE marking, perform risk assessments, and establish 10-year document retention.

In Scope, Lighter Steward Obligations (Article 24)	• Publishing FOSS without placing it on the market for direct commercialization. • Not-for-profit entities publishing FOSS, provided all revenue is reinvested into non-profit purposes. • Legal entities systematically providing sustained development support without direct commercialization.	**Steward Obligations**: Must document and implement a clear cybersecurity policy that encourages secure development, voluntary vulnerability reporting, and info-sharing.
Outside Scope Entirely	• Private individuals publishing software completely free of charge. • Offering optional, non-gatekept training, support, or consulting services separate from product access. • Accepting purely voluntary donations with no impact on product access or exclusive benefits.	**Exempt**: No compliance or reporting obligations apply under the CRA, provided no commercial activity is triggered.

MARTEL innovate

DIGITAL FOR PLANET

martel-innovate.com

digital4planet.org