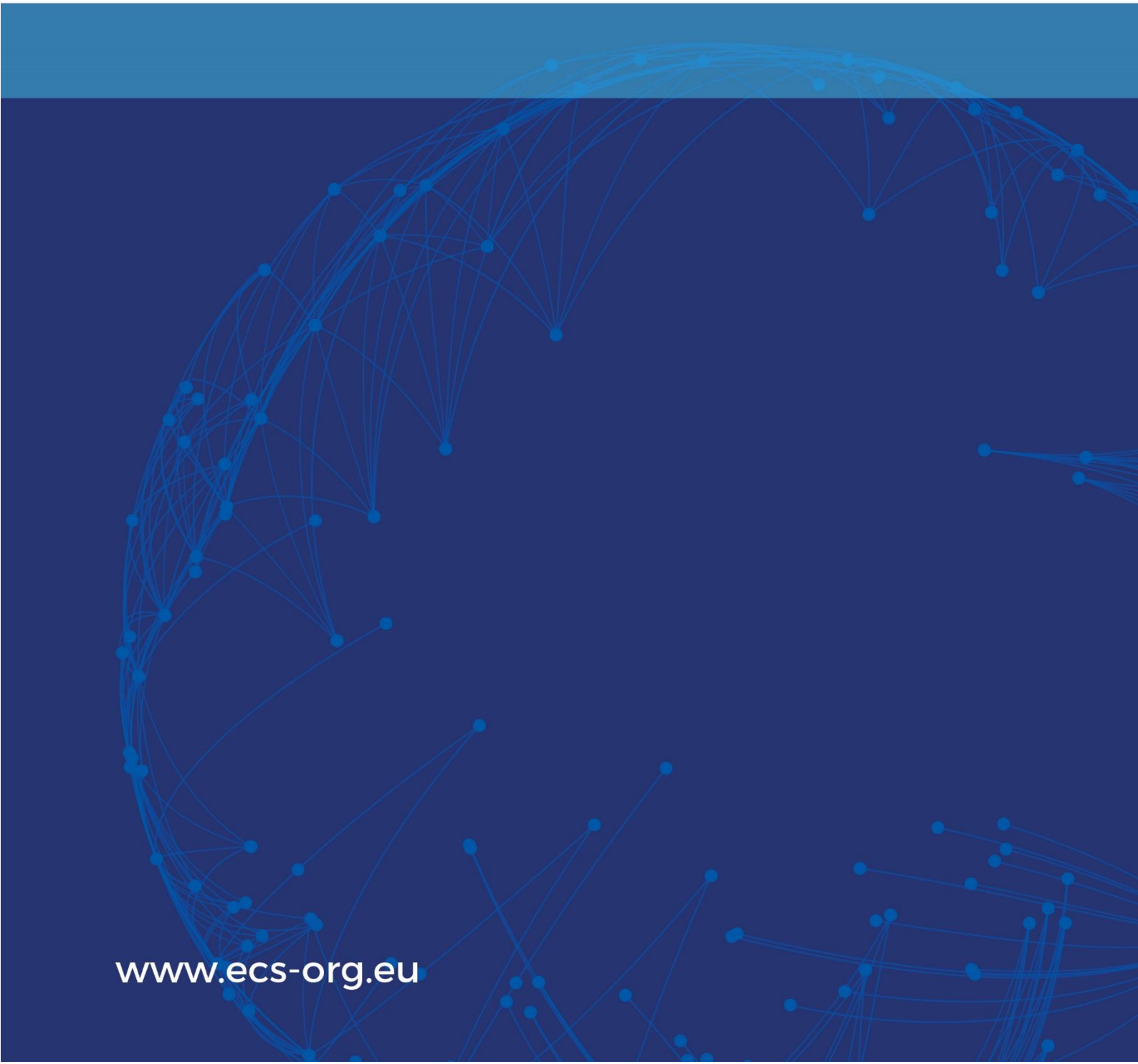
EUROPEAN CYBER SECURITY ORGANISATION

POSITION PAPER

Cyber Resilience Act

ECSO Working Group 1 and Policy Task Force

December 2022



www.ecs-org.eu

ECSO Position Paper on the Cyber Resilience Act

Executive summary

The **European Cyber Security Organisation (ECSO),** representing the backbone of the European cybersecurity ecosystem, welcomes the ambitious proposal for a Cyber Resilience Act (CRA). In this peculiar moment when the European Union is facing significant strategic cyberattacks by state and non-state actors threatening public and private systems, ECSO's Members are proud to contribute to the digital security of EU citizens, companies, and infrastructures. ECSO supports the work done over the years by the European Union to secure the European Digital Single Market with legislations and investments, and continues to advocate for more **European Strategic Autonomy**, **Digital Sovereignty**, and **Cyber Resilience**.

ECSO has consulted with its diverse members' base on the CRA and came forward with the following position paper. ECSO Members welcome the proposal of the CRA and support its objective; at the same time, they provide suggestions to the co-legislators to ensure that its implementation would not impose unnecessary burden to the European industry.

ECSO asks **guidance** to the European Union on **how companies should comply with this regulation**, especially when there is an interplay with other legislations like the Cybersecurity Act, NIS2 Directive, DORA, AI Act, and others. ECSO believes that a thorough mapping of global existing criteria and standards for conformity assessment should be done for the benefit of both the users, the producers, and the third-party certifiers.

The European cybersecurity industry needs to have a proper understanding of how products will be categorised, knowing in advance whether their products will fall under the default category, Class I or Class II. For this reason, it is essential for companies to have a clear **methodology for risk assessment and product categorisation** so that they can adjust their internal processes and invest for the right conformity assessment methods.

ECSO supports European **small and medium enterprises** and asks the co-legislators to consider how CRA will affect SMEs to ensure that the implementation will be manageable for all. The CRA will strengthen the security of the whole supply chain; for this reason, manufacturers of products with digital elements will save money as they will purchase more secure products from suppliers that will also be CRA-compliant. At the same time, the CRA will require investments from companies to comply with its obligations. As every company is unique, it is impossible to predict exactly the impact of this cost redistribution. To minimise its impact on SMEs, ECSO recommends **aligning the CRA with existing EU legislation** – like the Cybersecurity Act, NIS2 Directive, DORA, AI act – whenever possible and **provide guidelines** and **financial support to** help SMEs to better comply with the CRA.

Regarding reporting obligations, to minimise the burden on companies, the CRA should be **aligned with the NIS2** Directive and establish a **24-hour** deadline for **early warning** and **72-hour** deadline for **notification.** Ideally, the reporting should be done to the same entities. The interplay between the CRA and other legislations should also be clarified, promoting harmonisation wherever possible.

CHAPTER I – General provisions (Art. 1-9)

ECSO supports a **broad scope** of the CRA for both hardware and software and believes that products like endpoint Software as a Service solutions should also be included the scope. This is because of the increased use of cloud in the digital transformation and the fact that more products are being designed, created, and operated in a cloud environment.

Regarding the interplay with other legislations, ECSO asks the co-legislators to **clarify the overlaps with all other more vertical and sector-specific legislations** in order to facilitate compliance. Therefore, the link with the Network Code on Cyber Security (NCCS) for the electricity sector, the European Health Data Space regulation, the NIS2 directive, the Cybersecurity Act, the delegated Act on the Radio Equipment Directive, and DORA package should be made clear. The European Commission should provide **guidelines** to companies to understand what **requirements** they have to comply with and to whom they have to **report**.

With reference to **Art.3** on definitions, ECSO advocates for the following adjustments:

- Art.3(15) "*endpoint"*: cloud-deployed assets like apps, websites, etc., need to be included not only devices. Regulation (EU) 2019/1020 refers to "online interfaces".
- Art.3(37) "*software bill of materials"*: harmonised standards for software bill of materials are needed to make it readable, comparable, and transferable in both human and machine-readable format.
- A definition of *"cybersecurity incident"* should be inserted.

Regarding **Art. 4** on **free movement**, ECSO proposes to add the case of product development, amending Art.4(3) with the ensuing text "*Member States shall not prevent the making available of unfinished software which does not comply with this Regulation provided that the software is only made available for a limited period required for testing* ***or development*** *purposes and that a visible sign clearly indicates that it does not comply with this Regulation and will not be available on the market for purposes other than testing* ***or development***."

With reference to **Art.5 R*equirements*** *for products with digital elements,* ECSO considers that Art.5(1) is formulated in a way that adds unneeded confusion to the legal text. It would be sufficient for the Regulation to state: "*Products with digital elements shall only be made* ***available on the market where they meet the essential requirements*** *set of in Section 1 of Annex I*".

To better fit the market reality, a product with digital element should be **compliant** with the CRA at the **moment it is sold on the market and when it receives security updates** from the throughout its life cycle. The user should be allowed to freely customise the product according to their needs, and the producer should not be held liable for any security incident following customisations outside the contractual agreement.

CHAPTER II – Obligations of economic operators (Art. 10-17)

Regarding **Art. 10** on obligations for manufacturers, ECSO stresses that the indication of five years appears approximative considering the unique life cycle of each product. In this regard, ECSO proposes, at least for critical products that fall into Class I or Class II categories, that manufacturers provide **security updates for the entire product life cycle**, which is to say a timeframe that might exceed the 5 years, as it is usually the case for Operational Technology (OT). ECSO also asks for clarification on the definition of product cycle and how legal liabilities would articulate throughout the supply chain. It is important for producers to know what would happen if one component used in their supply chains arrives at the end of its expected life cycle.

We suggest letting the manufacturers decide about the length of the product life cycle for which they will provide security patches, with a minimum period of 5 years. This information should be indicated in the technical documentation (Annex V). Manufacturers should also give this information to the potential users before the product or service is sold.

When it comes to **reporting obligations**, ECSO believes that the CRA should envisage an **alignment with the NIS2 directive**. This would translate into **24-hour** deadline for **early warning** and **72-hour** deadline for **notification.** Furthermore, the regulation should have a provision for **confidential reporting to ENISA**. This is of particular importance for the industry because it often happens that a manufacturer is aware of a vulnerability but has not yet found a technical way to patch it. Finally, for every report and notification that a manufacturer sends to ENISA, a response shall be given without undue delay to inform the manufacturer that its report has been well received and to follow up on the next steps.

ECSO would also like to highlight the fact that entities belonging to the **financial sector** are already falling under the scope of DORA and NIS2 and would risk undergoing multiple reporting obligations for security incidents, having to report to ENISA (CRA), the national authorities (NIS2), and the financial supervisors (DORA). A similar situation exists also for the **energy sector** that falls both under the scope of the NIS2 directive and the Network Code on Cyber Security. These situations should be clarified with **dedicated guidelines and harmonisation** promoted whenever possible.

The current text obliges producers to make available and disseminate patching free of charge. In the **industrial sector**, while patching is usually made available free of charge, the criticality and complexity of industrial systems and installations have created a situation for which personalised services to clients to push the patching are sold separately. It follows that, the mandatory patching **should be free of charge at least for the last version of the product or service. The personalised service to push and install the patch in an industrial environment could be commercialised** under contractual agreement if the user needs assistance or external support in pushing the patches. Other similar business models – where the paid support to old versions supports the development of new ones – should be safeguarded. ECSO therefore encourages the co-legislators to clarify the text on **the definition of "disseminated"** (Annex I (8)), restricting it to the **provision of the patch** and not to its installation on the product, which is subject to the specifications of the industrial process and user choices.

In **Art. 10(1)** and **Art 10(4)**, it is important to state to what extent the manufacturer is responsible for the **supply chains** of its products. The text should specify the level of due diligence required and the responsibility that can be transferred to suppliers.

Art. 10 (5) refers to the need to **update the risk assessment** of the product by keeping into account new vulnerabilities and security incidents. A clarification is needed to understand whether the update should be internal, or whether the manufacturer shall provide the update to third parties.

Regarding **Art. 10(6)**, **Art. 10(8)** and **Art. 10(14)**, further text needs to be added to explain what would happen to a product with digital element in case its **manufacturer ceases their economic activity** due to liquidation or other reasons. In this scenario, it would be evident that the manufacturer would not be able to provide the support for the rest of the product life cycle and would not be in a position to report to ENISA about cybersecurity incidents and vulnerabilities. Furthermore, it is not clear what would happen to the technical documentation that is supposed to be stored for a period of ten years. ECSO invites the co-legislators to clarify these points in a way that would minimise the impact on companies and especially SMEs.

In **Art. 13(6)**, for the words **"vulnerability"**, **"active vulnerability"**, and "incident", ECSO suggests aligning the language with Art.10 on obligation for manufacturers.

Regarding **Art. 14(3)** and **Art.14(4)**, ECSO suggests clarifying the wording on **"significant cybersecurity risk"** and **"vulnerability"**.

CHAPTER III – Conformity of the product with digital elements (Art. 18-24)

Regarding the interplay with existing industry standards on cybersecurity, a thorough **mapping of all existing global standards** is required to better identify those that could be applied to the CRA. The European Commission should map existing standards and update the list of applicable ones regularly. Furthermore, the European Commission should create additional cybersecurity certification schemes under the EU Cybersecurity Act to facilitate compliance with the CRA.

We would therefore encourage the European institutions to take the long-term industry cyber security investment into account and to value it by creating a **compatibility mechanism**. This compatibility mechanism should rely on already adopted European industrial security standards framework (**EN IEC 62443**) including associated available IACS certification schemes operated by accredited European Conformity Assessment Bodies (CAB) actors.

In addition, the referred cybersecurity ecosystem allows European industry to have an **international reach and market recognition inside and outside Europe** for their products with digital elements.

CHAPTER VII – Confidentiality and penalties (Art. 52 and 53)

Regarding **Art. 53** on Penalties, ECSO proposes a **harmonious application of the fines** in every Member State and under the same conditions. All the national authorities should therefore apply the same rules in the same way, without any divergence or uncertainty as it is the case for the General Data Protection Regulation (GDPR). Very precise guidelines shall be provided to the national authorities in order to ensure a **level-playing field** in the European single market.

ANNEXES OF THE CRA– Annexes I-VI

Annex I Essential Cybersecurity Requirements

To date, Annex I.2 of the CRA reads: "***Products with digital elements shall be delivered without any known exploitable vulnerabilities***". ECSO invites the co-legislators to clarify the definition of known exploitable vulnerabilities by saying that these would the ones contained in **the EU vulnerability database to be set up by ENISA**, in accordance with the NIS2 Directive. Furthermore, ECSO stresses the importance of mentioning the notion of "**vulnerability handling" in the main text of the Regulation** and not only in Annex I.2.

Regarding the obligation to provide a "(…) ***possibility to reset the product to its original state***," ECSO indicates that there might be a correlated risk. More precisely, by using this function, the user would actually downgrade the product to a more vulnerable state, *de-facto* eliminating all the security patches and therefore involuntarily creating an attack vector. In addition to the above, an attacker could remotely reset a product to its original state, hence creating additional security risks. Should the co-legislators decide to keep the aforementioned obligation, it would be of utmost importance to **specify that the indicated possibility could only be executed while having physical access to the device** and under the full responsibility of the user. Any product with digital element must **keep logs for every customisation, patch, and update received and for any modification to its original state**.

Annex VI Conformity assessments

It is important that a company's confidential information does not become public without consent during the conformity assessment procedure. For this reason, under EU-type examination, based on Module B section 5, additional text should be added to state that **confidential information or trade secrets** of the manufacturer shall be kept confidential and used only by the third-party certifiers to assess the compliance.

Finally, in relation to conformity based on full quality assurance under Module H section 3.3 and 4.3, ECSO highlights that further details shall be envisaged in order to emphasise that any confidential information or **trade secrets of the manufacturer shall be kept confidential**.

Other recommendations

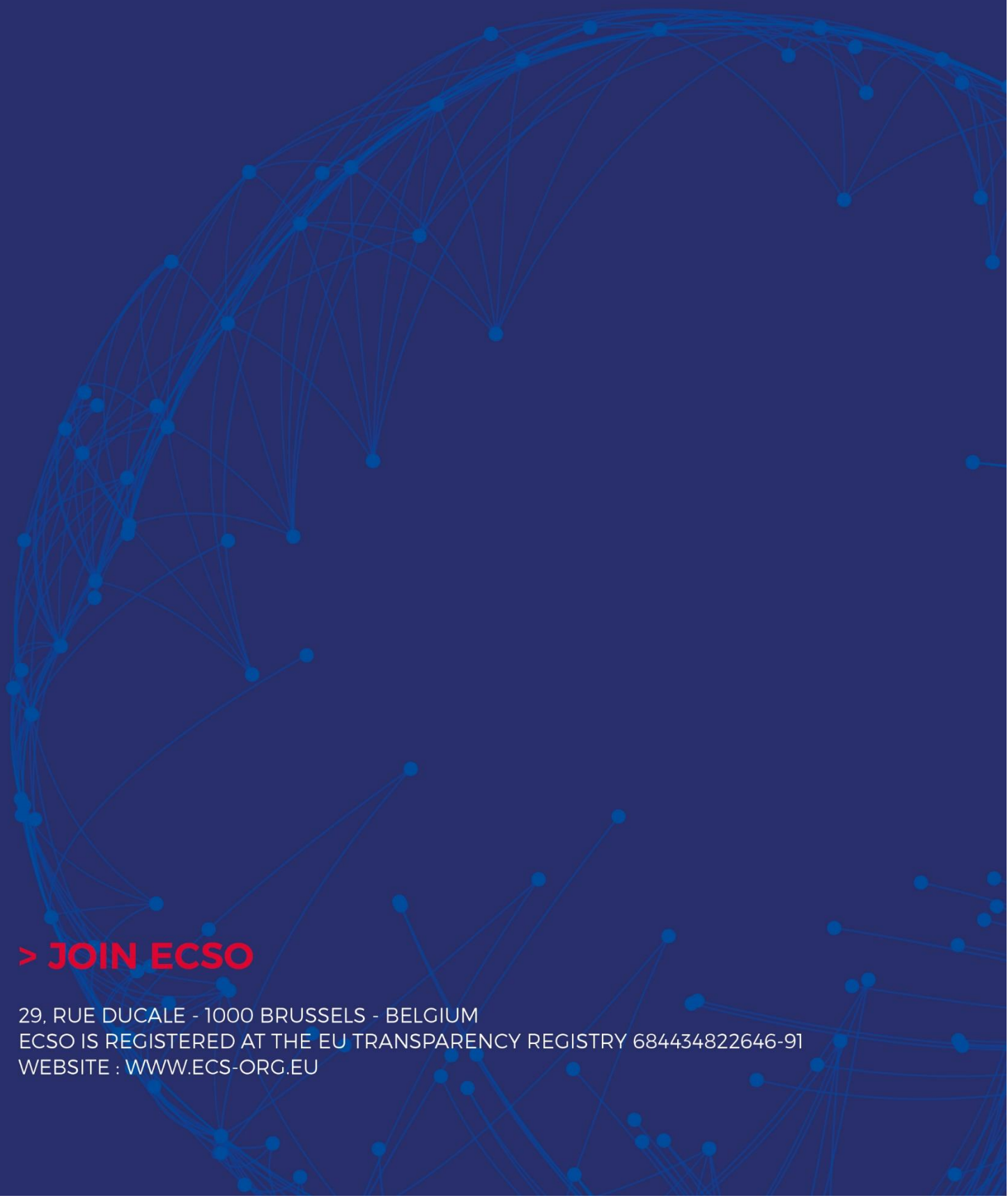
ECSO strongly supports the idea that all the IoT vendors – not only software but also hardware manufacturers – should adopt an efficient **DevSecOps** approach, including **Vulnerability Disclosure Policy (VDP)** as horizontal cybersecurity requirement for all digital products and ancillary services that are placed on the European market. The above-mentioned procedure should cover the **whole life cycle of the product**. Adopting a vulnerability disclosure policy facilitates the emergence of collective cybersecurity responsibility which will increase the trust in the digital market. The European Union through the CRA should propose a harmonised approach for the use of VDP and incentivise supply-side actors in treating vulnerabilities more effectively. ECSO would welcome **economic and legal incentives** to the use of VDP solutions implementing global standards as the ISO/IEC 29147 ("Vulnerability Disclosure") and ISO/IEC 30111 ("Vulnerability Handling") standards.

Contact persons

For any questions or comment feel free to contact:

- Francesco BORDONE – Junior Manager for Cybersecurity Policies, Legislation and Markets
  Email francesco.bordone@ecs-org.eu T: +32 492 11 36 72
- Costanza PESTARINO – Junior Manager for Supply Chain and Strategic Autonomy.
  Email costanza.pestarino@ecs-org.eu T: +32 492 11 40 48

ECS
EUROPEAN CYBER SECURITY ORGANISATION



> JOIN ECSO

29, RUE DUCALE - 1000 BRUSSELS - BELGIUM
ECSO IS REGISTERED AT THE EU TRANSPARENCY REGISTRY 684434822646-91
WEBSITE : WWW.ECS-ORG.EU