DIGITALEUROPE

24 JULY 2024

Developing guidelines for the Cyber Resilience Act

Executive summary

The Cyber Resilience Act (CRA) will for the first time introduce mandatory EU-wide cybersecurity requirements for all hardware and software products.[1] If implemented right, it will provide a clearer regulatory framework for cybersecurity of connected devices.

The CRA can increase Europe's cyber resilience, but for this to happen, certain elements must be made actionable for manufacturers, users and authorities. Recognising the complexity of its legal provisions, the CRA stipulates that the European Commission shall develop guidance to support authorities and the market in interpreting the text, including through consultation with industry.[2]

In this paper, we put forward concrete recommendations for issues that need to be addressed in the upcoming guidelines, including beyond those set out explicitly in the CRA:

- **Software as a product**: The CRA applies New Legislative Framework (NLF) concepts to software,[3] yet there are significant distinctions between tangible products and software. Placing software on the market requires not only making it available for download, but also transferring usage rights and providing access to it. Agreeing to a licence without payment, common with free and open-source software (FOSS), should not constitute placing it on the market.

[1] The CRA is awaiting publication in the Official Journal of the EU (OJEU) and will enter into force 20 days later, most likely in autumn 2024. We base this position paper on the final text voted on by the European Parliament (European Parliament legislative resolution of 12 March 2024 on the proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (COM(2022)0454 – C9-0308/2022 – 2022/0272(COD)). References to articles use the numbering in this version.

[2] Art. 26 CRA. We understand the Commission's intention is to complete this process at least a year prior to the CRA's implementation deadline to provide vendors time to prepare compliance.

[3] https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en.

DIGITALEUROPE
Rue de la Science, 37, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

- **FOSS**: Upstream open-source organisations are not considered manufacturers under the CRA. However, FOSS can be classified as a product once it enters commercial circulation. To clarify this, we suggest examples of activities that should not be deemed commercial. The CRA's focus on making products available in the EU poses challenges for FOSS, given its less controllable regional scope. The guidelines should restrict this concept to ready-to-use open-source packages for commercial use, specifically targeting companies integrating or offering open-source products in the EU market. The introduction of open-source stewards provides flexibility to accommodate the unique nature of FOSS, and we propose several ways in which the guidelines could support stewards.

- **Remote data processing**: The CRA excludes cloud-based solutions, yet lacks clarity on when these services fall under its scope. The guidelines should explicitly state that remote data processing, including cloud solutions, isn't classified as a 'product with digital elements.' To be considered part of a product, such processing must be essential for its functions and developed by the product's manufacturer. Scope should be limited to bidirectional data exchanges directly enhancing product functions, excluding services solely receiving data or not interacting directly.

- **Substantial modification**: Rules governing substantial modifications must be straightforward to ensure practical application of the CRA without requiring extensive legal analysis for each update. By default, security updates alone should not constitute a substantial modification. Similarly, upgrades should not automatically trigger substantial modification unless new risks arise. We propose simplified conformity assessments for substantial modifications when risks are sufficiently mitigated.

- **Support period**: Defining the support period should balance consumer expectations with practical constraints. Manufacturers should determine this period, with exceptional cases open to challenge only based on clear evidence. Flexibility in communicating support duration should be provided, ensuring consumer understanding.

- **Vulnerability handling**: The guidelines should clarify that patches are necessary only for vulnerabilities impacting product security in intended use. They should also clarify that effective vulnerability handling can serve as an appropriate mitigation whenever products cannot be updated remotely by the manufacturer to remedy known exploitable vulnerabilities prior to making them available on the market.

- **Vulnerability reporting**: The notion of 'becoming aware' should align with existing language in the European Data Protection Board (EDPB)

guidelines on personal data breach notifications.[4] 'Severe incidents' under the CRA should correspond to the definition of 'significant incident' under the Directive on measures for a high common level of cybersecurity across the Union (NIS2) and its interplay with the definition of special categories of personal data in the General Data Protection Regulation (GDPR).[5] The guidelines should minimise vulnerability reporting obligations for legacy products.

- **Interplay with other legislation**: Potential overlaps with other regulations need clear guidance to avoid duplicate reporting in line with the once-only principle.[6] Overly crowded cybersecurity reporting has been identified as a significant impediment to EU competitiveness in our recent report *The Single Market Love Story*.[7] The guidelines should provide a reporting template applicable across all relevant legislation.

We urge that guidelines should be developed alongside the secondary legislation foreseen in the CRA, notably the Art. 7(4) delegated act on the technical description of the categories of important and critical products in Annexes III and IV.

Table of contents

[4] Guidelines 9/2022.

[5] Directive (EU) 2022/2555 and Regulation (EU) 2016/679, respectively.

[6] In addition to NIS2 and the GDPR, these include the Radio Equipment Directive (RED) cybersecurity delegated act, the Digital Operational Resilience Act (DORA) and others, as we discuss in the 'Interplay with other legislation' section.

[7] See DIGITALEUROPE, *The Single Market Love Story: 10 digital actions to save the 30-year marriage*, available at https://cdn.digitaleurope.org/uploads/2024/02/DIGITAL-EUROPE-THE-SINGLE-MARKET-LOVE-STORY-FINAL-WEB.pdf.

Software as a product

The CRA regulates software on a large scale and applies NLF concepts to it. Even though the Medical Device Regulations have recognised software as a product for several years, this has only concerned applications with a specific medical purpose.[8] Similarly to the CRA, it is only recently that the revised Product Liability Directive and the AI Act have expanded the scope of EU product law to include software at scale.[9]

Given that the CRA is purpose agnostic, guidance is needed to elaborate on how NLF concepts should be understood for software products.

According to Art. 3(4) CRA, software is computer code being part of an electronic information system. The guidelines should specify that the code must be executable, which can be as low-level programming (e.g. object code, machine code or assembly language) or high-level programming language (source-code non-compiled but ready for compilation or interpretation). This does not include sample or demo code, or comments and other information provided with source code, as these are not intended to be used as software.[10]

Placing/making available on the market

We suggest transferring the Blue Guide's acknowledged key concepts of placing on the market to software as detailed below.[11]

Placing on the market is the first-time making a (unit of a) product available on the EU market. For tangible products, the Blue Guide explains further that placing a product on the market requires two conditions:

- The manufacturing stage has been completed; and
- An agreement (written or verbal) must be established between two or more legal or natural persons for the transfer of ownership, possession or any other property right.

For software, this would mean:

- The software needs to be provided (for download or on a data carrier for use by a person in the EU market); and
- The person needs to acquire the use rights for the software as well as the ability to access, possibly compile and use the software.

[8] Regulations (EU) 2017/745 and 2017/746.

[9] COM/2022/495 final, awaiting publication in the OJEU following trilogue agreement, and Regulation (EU) 2024/1689, respectively.

[10] See 'FOSS and open-source stewards' section.

[11] 2022/C 247/01.

A key difference between software and a tangible product is the issue of identifying individual units. The same unit of a tangible product cannot be placed on the market a second time; it can only be made further available. In contrast, the same software code or binary can be repeatedly placed on the market by the same legal entity. However, if a new entity acquires the software along with its property rights and resells it, the software is made available again under the new entity's property rights. Therefore, a unit of software is inherently linked to its access and usage rights.

Another consequence is that placing software on the EU market implies that at least one person, specifically the one acquiring the access or property rights, is situated in the EU. This concept, however, is challenging for FOSS, where the user is not necessarily known to the provider. This is one reason why agreeing to a licence without any associated payment should not be considered as placing the software on the market.

FOSS and open-source stewards

Whilst the concept of software as a product is already complex, it is even more crucial for FOSS that legal requirements align with technical and operational best practices. DIGITALEUROPE therefore welcomes the legal distinction made by the CRA between 'upstream' and 'downstream' FOSS. The CRA's general principle is that 'upstream' FOSS, meaning software created by commercial or non-commercial entities/individuals in FOSS communities, is either: a) fully exempt; or b) subject only to certain stewardship obligations (Art. 24).

Furthermore, the CRA clearly states that even when FOSS is eventually 'monetised' and integrated into or deployed as a 'product placed on the EU market,' it remains a special product since customers and users can access and scrutinise the FOSS code. Due to this FOSS-enabled transparency, under Art. 32(5) the CRA allows FOSS manufacturers to self-assess product categories listed under classes I and II of Annex III.

Important elements for FOSS organisations

The general principle is that upstream open-source organisations are not considered manufacturers. However, open-source organisations are highly diverse – ranging from foundations to entities and individuals creating solutions that qualify as digital public goods – so it is important to establish clear guidelines regarding their forms and structures.

Guidance, including examples and case studies, must offer legal clarity to open-source organisations that may simultaneously act as manufacturers and open-source stewards. As stewards, they are not obligated to meet requirements under Art. 13. Instead, their role is to assist downstream customers or users in fulfilling their due diligence obligations under Art. 13(5), for example, by participating in voluntary security attestation programmes (Art.

25) that enable the FOSS community to assess their products' conformity with the CRA.

Therefore, we suggest the guidelines clearly specify that upstream FOSS organisations can, in some cases, also be considered manufacturers, regardless of their legal form or structure. Additionally, the guidelines should clarify the circumstances in which a FOSS organisation would be regarded as a downstream organisation, such as when selling their products. In the next section, we provide respective suggestions.

Commercial activity

The upcoming guidelines should provide more examples of activities that should not be considered commercial activities by private organisations, as the current CRA text does not fully address this:

- **Upstream open-source projects:** An upstream open-source project is the source repository where contributions occur, and artifacts are made available under a FOSS licence. It should be clarified that only the downstream usage and market deployment of open-source projects in commercial software fall under the CRA.
- **Sample code/demo code published under open-source licences:** This type of code, often part of tutorials or training materials, should be explicitly mentioned. Companies may publish this code for others (customers, partners, etc.) to use as a template or inspiration, with the expectation that it will be adapted and not used unchanged by the consumer.
- **Outdated/archived FOSS projects:** These are open-source projects that have reached the end of their lifecycle or have been abandoned (e.g. maintainer leaves, company goes out of business). Although they are no longer maintained, they remain publicly visible for documentation purposes and for those who may want to continue working with them (e.g. fork/copy and restart maintenance and feature development). Such projects might no longer be suitable for productive use, and should only be used with additional risk mitigation measures.
- **Academic paper materials:** It is common for academic papers to include related data and/or code as a point-in-time support for the paper's conclusions. This allows other researchers to verify the conclusions by following the same path as the authors. Modifying this content for reasons outside of the paper, such as applying security fixes, can alter the original conclusions. Therefore, repositories of this data and/or code are usually left unedited and should not be treated as artifacts requiring ongoing maintenance.

The guidelines, developed in consultation with industry experts who contribute upstream, should provide additional examples to clarify cases where FOSS is developed without commercial activity.

DIGITALEUROPE has cautioned against using the NLF term 'commercial activity' to characterise FOSS monetisation, as it fails to fully capture the diverse and evolving business models within the open innovation ecosystem.[12] This mischaracterisation risks unintended consequences for products that qualify as FOSS but are intended for commercial activities. Including the 'intent' to monetise further risks undermining companies' willingness to support and allocate resources to their contributions to upstream open-source development, as their ultimate goal is typically to generate profit.

Placing/making available on the market

Defining FOSS as 'made available' in Europe is not straightforward. Unlike proprietary software, where ownership or access rights are transferred with each instance of making it available, FOSS is typically accessible globally as soon as it is published on platforms like GitHub, GitLab, etc. Vibrant communities span across the EU, contributing to and relying on global code repositories and collaboration platforms.

The guidelines should clarify that FOSS is inherently global and should not be localised regionally. Any attempt to localise such development would fragment production and severely disrupt open innovation.

The concept of 'making it available' should specifically apply to ready-to-use open-source packages offered on platforms (via repositories) for commercial use. Providers in this context should be recognised as OSS stewards rather than manufacturers. This distinction reflects the asymmetric nature where the licence provider has limited control over how the licensee may commercially utilise the software.

Open-source software can be made available in different forms:

- As **source code** via developer platforms like GitHub and GitLab, or via self-hosted platforms. In this form, users/consumers must build the software themselves. Therefore, the source code provider cannot regulate or control the environment or outcome of this build process. FOSS consumption in this manner requires higher effort from the user.
- In **'packaged form'/as binaries**, distributing pre-built packages or artifacts resulting from a build process. Consumers do not need to build the software themselves, and the package provider has some ability to

[12] See DIGITALEUROPE, *Building a strong foundation for the Cyber Resilience Act: Fey considerations for trilogues*, available at https://cdn.digitaleurope.org/uploads/2023/09/DIGITALEUROPE_Building-a-strong-foundation-for-the-CRA_key-considerations-for-trilogues.pdf.

regulate its use. Platforms such as Maven Central, PyPi and npmjs offer such pre-built packages for easier consumption.

Including these general-purpose platforms would pose a significant risk to entire ecosystems and would not align with the CRA's objectives. It would be more effective to focus regulatory efforts on companies that integrate or offer open-source products specifically on the EU market, where their commercial interests are clear. Packages licensed under free and open-source terms on widely recognised publishing platforms for source code and package managers (should be explicitly exempted from regulatory requirements by the guidelines.

Furthermore, it's important to note that a manufacturer has limited control over whether its product is placed on the EU market directly by the customer or through a third party, especially if it was initially placed on a non-EU market. The guidelines should provide specific scenarios or examples that address product placement on the EU market through second or third parties, including associated obligations. This clarity will help ensure consistent compliance and understanding of regulatory requirements across different market entry scenarios.

Open-source stewards

Swift support for FOSS stewards will be crucial. The proposed attestation programme (Art. 14b) will need to be developed by the Commission. Additionally, FOSS stewards will be required to formulate a cybersecurity policy, which will also require further guidance from the Commission.

It would be beneficial to reference recommended standards such as ISO/IEC 30111 and ISO/IEC 29147, alongside future harmonised standards for vulnerability handling and reporting, to provide comprehensive advice for FOSS stewards.

The guidelines should particularly aid FOSS stewards in understanding the distinction between liability for damages and market access obligations, especially concerning protecting developers under FOSS licences and utilising mutual recognition for potential third-party certification instances.

Moreover, as roles in the FOSS supply chain are not always clear-cut, future CRA conformity guidance for stewards should not differentiate between private individuals/projects and not-for-profits. Instead, it should focus on demonstrating capabilities through conformity assessments based on quality assurance programmes, best practices for control procedures (e.g. maintaining reasonable response times to mitigate vulnerabilities), rather than requiring commercial-grade service level agreements (SLAs).

Furthermore, the guidelines should emphasise the importance of downstream users of stewards' packages and projects engaging with and informing stewards about potential vulnerabilities. This is crucial due to the diverse nature of the upstream community, which includes those who maintain packages with

minimal coding experience as well as developers actively contributing to the packages they maintain, fostering rapid innovation cycles within the ecosystem.

To further operationalise the concept of stewards, DIGITALEUROPE proposes the following initial guiding approaches for guidance related to open-source stewards:

- **Organisational governance**: Private companies or their subsidiaries should be eligible for 'open-source steward' status if they oversee open-source projects without direct commercial interests (upstream projects). If the concept extends to natural persons, project maintainers could also fulfil these roles, given their existing responsibilities such as managing vulnerabilities. It's essential to distinguish when a for-profit or not-for-profit entity transitions from stewardship activities to activities clearly defined as 'placing on the market' under the CRA guidelines. This transition would automatically subject them to CRA obligations, highlighting the importance of establishing a consistent level of stewardship governance to achieve a harmonised approach in fulfilling the objective of 'systematically providing support on a sustained basis.'
- **Legal framework**: Stewards should commit to maintaining sufficient legal hygiene by conducting necessary reviews of licensing policies to prevent non-open-source licences from entering collaborations.[13] The CRA's definition of 'openly shared' under recognised FOSS licences is a critical value that supports and encourages upstream open-source collaboration whilst reinforcing established principles of liability safe-harbouring.
- **Operational approach**: Best practices and steward attestations should adopt a standardised template to simplify due diligence requirements for downstream manufacturers, particularly SMEs. This approach aims to facilitate their engagement with open source and foster increased contributions to a more resilient supply chain through proactive upstream fixes. Similarly, cybersecurity policies for vulnerability disclosures should also benefit from standardised templates to support SMEs and companies less familiar with open source, thereby preventing inadvertent fragmentation of access to global commons.
- **Collaboration with regulatory authorities**: Open-source stewards are rightfully exempt from CRA penalties and specific obligations, but are obligated to collaborate with market surveillance authorities to implement corrective measures. Guidelines should clarify how these obligations can be fulfilled without penalties, potentially through model 'terms and references' for open-source stewards included in the guidance.

[13] As seen in the Cloud Native Computing Foundation's (CNCF) role within Kubernetes.

- **Support by European standards organisations**: The guidelines could encourage European standards organisations to develop standardisation related to the definition and best practices of open-source stewardship. Beyond the technical aspects, this initiative presents an opportunity to integrate expertise from the open-source community into European standardisation efforts.

Remote data processing

As product regulation, the CRA explicitly excludes services such as cloud-based solutions like software-as-a-service (SaaS), platform-as-a-service (PaaS) or infrastructure-as-a-service (IaaS). However, the CRA is ambiguous regarding the circumstances under which cloud-based services might still fall within its scope. Recital 12 references cloud solutions, stating they could be categorised as 'remote data processing' if they meet the definition outlined in the CRA.

To provide clarity, we recommend that the guidelines elaborate on the concept of remote data processing. Firstly, it should be explicitly stated that remote data processing, including cloud solutions such as SaaS, PaaS and IaaS, does not qualify as a 'product with digital elements.' This would avoid confusion regarding the regulatory obligations for cloud-based services versus physical products with digital components. Providers of remote data processing services should not be classified as manufacturers solely by offering data processing services.

Included data processing

Based on Recitals 11-12 and Arts 3(1)-(2), the guidelines should clarify that 'remote data processing' refers to processing that occurs outside the product with digital elements. This processing can be considered part of the product itself under two specific conditions:

- It must be necessary for the product to perform its functions.
- The software performing the processing must be designed and developed by the manufacturer of the product.

Given the diverse and evolving architectures in cloud computing, manufacturers must be given clear indications on scope. We strongly recommend limiting the scope to remote data processing that:

- *Directly* interacts with the product; and
- Involve a bidirectional exchange of data. This means data is sent from the product to a remote data processing service, and then the results are sent back to the product to enable one or more of its functions.

An example could be systems controlling an industrial robot, where a camera feed from the robot is sent to a remote service that calculates the position of a part based on the camera feed and sends control commands back to the robot to pick up a part. Here the robot, including the camera, is the product with digital elements. The remote service is part of that product. This service should not compromise the security of the robot. For example, the robot (and its driver software) needs to ensure essential requirements of Annex I.I.2e (confidentiality). This also concerns the data flow to and from the remote service which needs to be encrypted.

Product manufacturers will be required to consider remote data processing in their conformity assessments. Further consultations with cloud computing experts will be needed to ensure future conformity assessments are manageable. In general, we suggest more in-depth discussions with concerned stakeholders for further clarifications, as the Commission is already conducting on Annex III definitions.

Excluded data processing

Remote services that solely receive data from a product should not fall within the scope of remote data processing. Examples include services that receive log information from products for storage or those monitoring machine operations to alert technicians of wear signs. Similarly, any services not directly interacting with the product, even if the remote data processing solution interacts with them on the backend after receiving data, should be excluded.

Cloud services may include mobile applications accessing APIs or databases as part of their SaaS offerings. The guidelines should clarify that such mobile apps connecting to websites or cloud services do not qualify as products with digital elements, nor should cloud providers be considered manufacturers for providing such mobile applications. This clarification prevents cloud providers from facing overlapping obligations under NIS2.

Additionally, offline activities performed by a manufacturer, such as compiling software updates for a product, do not constitute remote data processing according to Art. 3(2).

Conformity assessment of remote data processing

The guidelines should provide additional clarity as to how manufacturers should incorporate the security of remote processing into their products' conformity assessments. Like the due diligence requirements imposed on manufacturers, those utilising open-source software should include remote services in their risk assessments and demonstrate how risks are adequately mitigated. It's important to acknowledge that achieving 100% security for every line of code involved in remote data processing is impossible.

Substantial modification

We endorse the principle outlined in the current definition of substantial modification in the Blue Guide, and advocate for its continued use as the guidelines' foundational basis for clarification. A modification should be deemed substantial if it meets all the following criteria:

- It changes the original performance, purpose or type of the product, which was not anticipated in the initial risk assessment;
- It alters the nature of the hazard or increases the level of risk concerning relevant Union harmonisation legislation; and
- The modified product is placed on the market.

Regarding cybersecurity, the handling of software updates is particularly critical. The Blue Guide identifies a software update as a substantial modification if:

- The update modifies the original intended functions, type or performance of the product without being anticipated in the initial risk assessment;
- The update changes the nature of the hazard or increases the level of risk associated with the product; and
- The updated product is made available.

Security updates

Security updates alone should not automatically be considered substantial modifications.

Recital 39 CRA clarifies that 'where security updates that are designed to decrease the level of cybersecurity risk … do not modify the intended purpose of a product with digital elements, they are not considered a substantial modification.' However, the same recital emphasises that 'where feature updates modify the original intended functions or the type or performance of a product with digital elements and meet those criteria, they should be considered a substantial modification,' thereby triggering a new conformity assessment.

Security updates must be implemented as promptly as possible. Prolonged delays in manufacturers' response to evolving cybersecurity threats would undermine product security and resilience, contrary to the CRA's overarching goals. Postponing the deployment of updates poses a greater risk than the potential theoretical increase in attack surface.

To avoid potential reluctance in issuing updates due to extensive legal analysis for each update, the guidelines should explicitly state that a security update alone by default does not constitute a substantial modification.

The guidelines, however, should recommend that all updates, including security updates, adhere to defined quality procedures to minimise the risk of unintended consequences. Additionally, comprehensive documentation of updates and any changes in the software bill of materials (SBOM) should be ensured to support transparency and traceability.

Upgrades

Upgrades do not automatically constitute a substantial modification. According to Recital 39, however, 'where feature updates modify the original intended functions or the type or performance of a product with digital elements and meet those criteria, they should be considered a substantial modification, as the addition of new features typically leads to a broader attack surface, thereby, increasing the cybersecurity risk.'

To provide clarity, the guidelines should differentiate between an 'update' and an 'upgrade.' An 'update' enhances a product's original functionality without changing its intended use, thereby never constituting a substantial modification by definition. Only 'upgrades,' which may potentially change a product's intended use, should be considered for a new risk assessment, particularly if the risks have increased, aligning with the principles outlined in the Blue Guide.

The pivotal consideration should always be the associated risks. Therefore, we propose that upgrades necessitate a new risk assessment only when there is a discernible increase in risks, a point that should be clearly articulated in the guidelines.

Furthermore, it is crucial to specify that the installation of third-party software by users (such as on computers or smartphones) should not be deemed a substantial modification, provided it was foreseen in the product's initial risk assessment. The responsibility for compliance with CRA requirements rests with the third-party software, which constitutes a product under the CRA.

Conformity assessment of substantial modifications

The guidelines should incorporate provisions for a streamlined conformity assessment process for substantial modifications under defined conditions.

When determining whether a software upgrade qualifies as a substantial modification, the guidelines should explore the possibility of allowing leniency in the application of a full conformity assessment if the associated risks are sufficiently mitigated.

If a new risk assessment is deemed necessary, the SBOM should be utilised to assess whether the risks introduced by the change are contained enough to warrant a shorter conformity assessment track.

It should be explicitly stated that no new CE marking is required if conformity with the CRA is maintained after a substantial modification, even in cases involving software.

According to the CRA, the declaration of conformity (DoC) must be updated to reflect substantial modifications, which can be digitally updated online. As per general CE regulations, where only one DoC is required across all regulations, the guidelines should clarify that updating the online version suffices, even for regulations that still mandate a physical, written DoC.

Lastly, to ensure coherence, the CRA guidelines should be aligned with those of other legislation such as the AI Act, the Machinery Regulation,[14] the General Product Safety Regulation (GPSR)[15] and the Product Liability Directive, which may define substantial modification slightly differently.

Support period

The support period is a critical concept in the CRA as it defines specific manufacturer obligations, particularly concerning vulnerability handling and technical documentation updates.

Conditions for determining the support period

The CRA outlines conditions for determining this period, balancing expectations like product lifetime with factual constraints such as component support periods or the availability of operating environments. This balancing act is crucial for products that combine physical and digital elements, where lifetimes can vary across different components.

The guidelines should emphasise that only manufacturers can determine the support period's length. It should be clarified that challenges to the manufacturer's determination should only occur in exceptional cases with clear evidence. According to the CRA, the dedicated administrative cooperation group (ADCO) should collect reliable evidence and highlight any discrepancies between manufacturer decisions and the outlined conditions.[16] This information should then be made public, providing recommendations for determining support periods across the EU. This approach ensures manufacturers' planning certainty and avoids unjustified challenges by authorities or stakeholders.

[14] Regulation (EU) 2023/1230.

[15] Regulation (EU) 2023/988.

[16] Art. 52(16).

To assist manufacturers in setting support periods, the guidelines should collect factual evidence on expected lifetimes, referencing Commission studies such as those available under ecodesign legislation.[17]

Additionally, the guidelines should highlight Recital 61, which clarifies that whilst security support periods should generally be at least five years, shorter periods may be justified for certain products, such as those tied to subscription expiration.

Support period end date

Regarding the CRA's requirement to communicate the end date of the support period,[18] achieving practical clarity for end-users poses a challenge. The end date can be communicated as an absolute date, which would appear the preferred interpretation under Art. 13(19) CRA. Alternatively, it could be communicated relative to the purchase date (e.g., six years and five months after purchase, akin to sales law guarantees) or five years after the last unit is placed on the market.

An absolute end date offers clarity to users and allows manufacturers control over their commitments, unlike a date relative to sales, which depends on market dynamics. This is particularly pertinent when importing components first made available outside the EU.

However, communicating an end date for each product unit (Annex II.7) may often underestimate the actual support period. Manufacturers must conservatively set a 'minimum end date' for legal certainty, potentially extending it if the model remains on the market longer. This is crucial for ADCO's evaluation of 'inadequate support periods,'[19] focusing on the actual support period rather than estimates. Clear communication is essential to prevent consumer confusion about the actual duration versus stated paperwork.

Vulnerability handling

The manufacturer's primary obligation during the support period is vulnerability handling.[20] The objective is to identify, evaluate and mitigate vulnerabilities based on their risk. Whilst this concept is well-established in cybersecurity, it is novel in NLF legislation to maintain product conformity beyond market placement.

[17] Regulation (EU) 2024/1781.

[18] Art. 13(19) and Annex II.7.

[19] Art. 52(16).

[20] Annex I – Part II CRA.

For clarity, the guidelines should emphasise that patches must be provided only for vulnerabilities posing a risk to the product's security in its intended use.[21]

Whilst automated or forced updates might be suitable for some products, it is crucial to note that the manufacturer's obligation is limited to providing the updates. This is particularly relevant for products that cannot be entirely updated remotely, such as production machinery or any product where the manufacturer does not have direct access.

The guidelines should state that the manufacturer's responsibility is to provide the update and inform the user according to Annex I.II(4) that an update is available. The responsibility for scheduling and installing the update lies with the product user.

The requirement in Annex I – Part I (2)(a) that only products without known exploitable vulnerabilities can be made available on the market is technically impossible for many tangible products in the supply chain, which typically cannot be updated remotely whilst packaged, stored and without power. The guidelines should clarify that these conditions may render the provision inapplicable, but effective vulnerability handling can serve as an appropriate mitigation. Additionally, the guidelines should offer solutions for manufacturers and distributors regarding conditions under which they may sell products with known vulnerabilities, such as ensuring effective vulnerability handling when the product is first put into service.

Vulnerability reporting

DIGITALEUROPE has consistently advocated for the principle of 'one incident, one report.' The guidelines should include a standardised reporting template applicable across various legislations where incidents must be reported, such as NIS2, the Digital Operational Resilience Act (DORA)[22] and the GDPR, among others. This template should provide a basic format with the flexibility to add more details as needed.

It is crucial to minimise the volume of reports to avoid information overload and ensure consistency in reporting during the dynamic process of an ongoing investigation. Reporting on exploited vulnerabilities will result in a higher number of reports, making it essential to streamline the information in each report.

The guidelines should also support the delegated acts that specify the procedures and criteria for actively exploited vulnerabilities. This ensures that

[21] This clarification is essential since Art. 13(8) and Annex I – Part II CRA refer merely to 'vulnerabilities.' The definition in Art. 3.(40), which pertains to cyber threats, combined with the definition of 'cyber risk' (Art. 3(37)) and the CRA's broader cybersecurity objectives, implies that only vulnerabilities posing a cyber risk need to be addressed.

[22] Regulation (EU) 2022/2554.

at every stage, the information remains restricted to prevent the reconstruction or creation of variants that could compromise the essential security interests of the EU and the global community.

For comprehensive final reports, we recommend adopting approaches like those used for CVE-2024-21312 .NET Framework Denial of Service Vulnerability[23] or CVE Record.[24]

Becoming aware

The guidelines should clarify the timing for the 24h/72h reporting requirements, emphasising that becoming aware of a vulnerability is a complex process that involves assessing whether the vulnerability poses a risk to the product in question.

It should be specified that the 24-hour period starts only after there is sufficient evidence that the vulnerability exists in the product and is actively being exploited. This approach should align with the EDPB guidelines on personal data breach notifications. According to these guidelines, a controller is considered aware of a breach when they have a reasonable degree of certainty that a security incident has occurred. The EDPB guidelines also state that after being informed of a potential breach, the controller may undertake a short investigation period to confirm whether a breach has occurred. During this investigation, the controller is not regarded as being aware of the breach.

For user information, the guidelines could recommend that manufacturers use a website to inform users about vulnerabilities, ensuring transparency and timely updates for users regarding potential security risks.[25]

Legacy products

Regarding the transitional provisions,[26] the guidelines should clarify that a product placed on the market before the end of the transition period can still be legally sold or put into service after the transition period. For instance, products already in stock at distributors' warehouses remain legal for sale even after the transition period has ended.

This provision is particularly relevant for handling vulnerabilities. Legally, vulnerability handling is not required for products placed on the market during the transition period. However, this exemption does not extend to vulnerability reporting. Reporting obligations apply to all products, regardless of when they were placed on the market. This creates challenges for legacy products that

[23] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21312.

[24] https://cve.mitre.org/.

[25] Similar to Microsoft's Security Update Guide, available at https://msrc.microsoft.com/update-guide/.

[26] Art. 69(2).

were placed on the market before the CRA came into effect and before the reporting obligations were established.

The guidelines should clarify that:

- **For products placed on the market before the CRA's application date, reporting is a 'passive' duty**. Manufacturers should not be required to actively search for or test for vulnerabilities in legacy products. They should only report incidents and exploited vulnerabilities they become aware of without active searching.
- **The level of detail required in reports for legacy products should be limited**. Manufacturers should not be expected to provide comprehensive reports for products that were not subject to these requirements when they were placed on the market.
- **In cases where the risk is low or the product is obsolete, non-reporting should be allowed**. This ensures that resources are focused on addressing more significant and current threats rather than outdated or low-risk products.

Severe incidents: alignment with other legal frameworks

The CRA's definition of 'severe incident' at Art. 14(5) differs from NIS2's use of 'significant incident.'[27] Similar to NIS2, clear criteria are needed to qualify something as a severe incident, based on severe operational disruption, financial loss or considerable damage to the user. Additionally, it is crucial to determine whether the data related to the incident is 'sensitive' or 'important,' yet these terms are not defined in the CRA text.

To address this, it is essential to provide guidance on the definitions of 'sensitive' and 'important' data. For example, customer credentials could be considered sensitive or important data. Alignment with existing legal frameworks such as the GDPR, where 'sensitive data' is understood as special categories of personal data,[28] would be beneficial. In practice, these concepts will often coincide.

For the elaboration of the guidelines, we suggest that the Commission and the European Union Agency for Cybersecurity (ENISA) collaborate with the US CVE Program to ensure comprehensive and coherent criteria for identifying and reporting severe incidents.[29]

Interplay with other legislation

[27] Art. 23(3) NIS2.

[28] Defined in Art. 9 GDPR.

[29] https://www.cve.org/.

It is important to recognise that other sectors have similar requirements to the CRA, with the same objectives. To prevent overlaps with other sectoral requirements, the guidelines should elaborate on the interplay between the CRA and the following regulations.

RED delegated act

As the CRA's application date approaches, companies are likely to ensure their products are compliant with the CRA in advance due to logistical reasons, particularly concerning large product portfolios and extensive supply chains. In cases where a product falls under both the CRA and the Radio Equipment Directive's (RED) cybersecurity delegated act,[30] and already complies with the former, DIGITALEUROPE believes the product should be considered compliant with both. This issue can ultimately only be resolved in a legally certain manner within the RED delegated act itself.

During the transition period, products should be deemed compliant with the RED delegated act if they meet the CRA requirements and fall within the scope of both. Before the RED delegated act is repealed upon the CRA's date of applicability, the CRA standardisation request should include the objective of reusing the RED standards when developing CRA standards. This will ensure a smoother transition and avoid unnecessary duplication of compliance efforts.

NIS2

There will be significant overlaps between the vulnerability reporting policies adopted by Member States under NIS2 and the CRA's vulnerability handling requirements. To avoid redundancy, the guidelines should clearly state that vulnerability reporting under the CRA should not result in double reporting and disclosure obligations compared to NIS2. The guidelines should stress the principle of once-only reporting to avoid double reporting obligations.

NIS2 provides a common framework for managing cybersecurity risks and incident reporting. In contrast, the CRA focuses on the cybersecurity of products. However, Member States can impose diverse national cybersecurity requirements, including for products throughout the supply chain, which would typically already be covered by the CRA. The guidelines should specify that NIS2 requirements are solely applicable to cybersecurity risk management in operations and services, whilst everything product-related is covered by the CRA. This distinction will help prevent duplication, market fragmentation and gold plating.

There is also a high risk of inconsistent compliance rules for software. As previously detailed, the CRA is not sufficiently clear on when cloud-based software tools constitute remote data processing solutions. As a result, they may fall under both the CRA and NIS2, despite these two targeting different

[30] Commission Delegated Regulation (EU) 2022/30 supplementing Directive 2014/53/EU.

aspects of the cybersecurity domain. Recital 12 CRA states that cloud solutions are subject to NIS2, but it does not clarify how this impacts their treatment under the CRA. Given that most products are backed by cloud services and the EU aims to further increase cloud uptake, this creates ambiguity regarding the applicable security requirements.

DORA

In the case of financial institutions, overlaps between DORA and the CRA are likely, despite the fact that DORA's objectives encompass and even exceed the CRA's. These overlaps are particularly expected in incident reporting. Financial institutions, such as banks, may find themselves required to submit multiple reports about the same cyberattack – not only to relevant authorities under DORA, but also to computer security incident response teams (CSIRTs) under the CRA if deemed necessary by such authorities. This double reporting would burden financial institutions and diminish the effectiveness of both legal regimes by diverting attention from managing the incident to complying with overlapping reporting obligations.

GDPR

The GDPR mandates that organisations notify data protection authorities (DPAs) of personal data breaches (Art. 33). If a company, acting as a controller of personal data (e.g. customer information), experiences a cybersecurity incident affecting privacy, it must report to both the relevant CSIRT under the CRA and the competent DPA under the GDPR.[31]

As previously highlighted, the guidelines should emphasise the principle of reporting only once, including in cases where cybersecurity incidents involve personal data breaches.

Furthermore, as also previously discussed, it is crucial to align the concept of incident or vulnerability awareness with EDPB guidelines pursuant to the GDPR.

Machinery Regulation

The Machinery Regulation's essential requirements aim to safeguard personal health and safety. In contrast, the CRA's essential requirements focus on ensuring the confidentiality, availability and integrity of data, along with the security of information assets such as network functionality.

Effectively, the CRA addresses potential causes that could lead to risks affecting health and safety. Specifically, the CRA addresses risks related to

[31] Additionally, as highlighted above, depending on the circumstances, reporting may also extend to other competent authorities under NIS2 or DORA.

'intentional corruption' and 'malicious attempts from third parties,' which overlap with similar risks addressed in the Machinery Regulation.[32]

The guidelines should clarify this relationship and recommend that the risk assessment under the Machinery Regulation and the applicable conformity assessment for these two essential health and safety requirements consider conformity with the CRA as sufficient mitigation against risks of 'intentional corruption' and 'malicious attempts from third parties' concerning software and data.

Medical Device Regulations

The Medical Device Regulations represent robust, comprehensive and up-to-date legal frameworks governing the medical technologies industry in the EU. The guidelines should emphasise the reuse of specific healthcare sector processes for applications and products falling under the CRA, and intended for use within healthcare provider environments and their value chains.

Additionally, the guidelines should acknowledge that electronic health record (EHR) systems will be indirectly impacted by the CRA. Sufficient time should be provided to adapt these systems to meet the advanced cybersecurity requirements outlined in the CRA. The guidelines should also elaborate on the CRA's interplay with the recently adopted European Health Data Space (EHDS) provisions covering elements specific to EHR systems.[33]

FOR MORE INFORMATION, PLEASE CONTACT:

- Rita Jonusaite
  Senior Policy Manager for Cybersecurity & Cloud
  rita.jonusaite@digitaleurope.org / +32 499 70 86 25
- Sid Hollman
  Policy Officer for Cybersecurity & Digital Infrastructure
  sid.hollman@digitaleurope.org / +32 491 37 28 73
- Milda Basiulyte

[32] Arts 1(1)(9) (Protection against corruption) and 1(2)(1) (Safety and reliability of control systems), respectively.

[33] The final EHDS text stipulates at Recital 73a that 'manufacturers may draw up a single technical documentation containing the elements required by both legal acts. It should be possible to demonstrate compliance of EHR systems with essential requirements laid down in [the CRA] through the assessment framework under [the EHDS]' (COM(2022)0197 – C9-0167/2022 – 2022/0140(COD)).

Senior Director for Cyber, Infrastructure & Competitiveness

milda.basiulyte@digitaleurope.org / +32 493 89 20 59

Alberto Di Felice

Policy and Legal Counsel

alberto.difelice@digitaleurope.org / +32 471 99 34 25

About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory environment that enables European businesses and citizens to prosper from digital technologies. We wish Europe to grow, attract, and sustain the world's best digital talents and technology companies. Together with our members, we shape the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies. Our membership represents over 45,000 businesses that operate and invest in Europe. It includes 108 corporations that are global leaders in their field of activity, as well as 41 national trade associations from across Europe.