DIGITALEUROPE

23 JANUARY 2023

Cybersecurity everywhere: deciphering the Cyber Resilience Act

Executive summary

Cybersecurity has become indispensable to our economy and society, and can no longer be an add-on to Europe's regulatory landscape for products. DIGITALEUROPE strongly welcomes and supports the objectives of the proposed Cyber Resilience Act (CRA), which will for the first time introduce mandatory cybersecurity requirements for 'products with digital elements.'[1]

DIGITALEUROPE has consistently advocated in favour of horizontal cybersecurity requirements for connected devices.[2] This is not only because of the heightened importance of securing the growing number of devices on the market, which are projected to reach 34.7 billion connections globally by 2028,[3] but also the increased risk of an unclear regulatory framework.

Recent years have seen a proliferation of piecemeal cybersecurity requirements under different EU laws.[4] This complex regulatory scenario is making compliance more difficult for companies, as well as authorities, which in turn will work against a more cyber secure posture in the EU.

The CRA can offer a long-term solution to help manufacturers, users and authorities strengthen cybersecurity across the board. For this to happen, however, we must consider measures that make compliance clear and actionable rather than generate new uncertainty.

An effective CRA must:

[1] COM(2022) 454 final.

[2] See DIGITALEUROPE, *Setting the standard: How to secure the Internet of Things*, available at https://www.digitaleurope.org/wp/wp-content/uploads/2021/09/DIGITALEUROPE_Setting-the-standard_How-to-secure-the-Internet-of-Things.pdf.

[3] *Ericsson Mobility Report*, November 2022.

[4] For a non-exhaustive overview of existing or proposed EU laws stipulating cybersecurity requirements for products or entities, see pp. 4-5, DIGITALEUROPE, *Building blocks for a scalable Cyber Resilience Act*, available at https://www.digitaleurope.org/wp/wp-content/uploads/2022/05/Building-blocks-for-a-scalable-Cyber-Resilience-Act.pdf.

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

- **Factor in the specificities of standalone software**, such as the impact of software updates on old concepts such as 'substantial modification,' including through the development of **guidelines with input from a newly created Stakeholder Expert Group**, which should advise the Commission on the CRA's implementation and future review;
- **Exclude hardware, software and services used for remote data processing, transmission and storage**, to avoid excessive overlap with the new Directive on measures for a high common level of cybersecurity across the Union (NIS2);[5]
- **Introduce the concept of 'partly completed product with digital elements,'** allowing for more accurate conformity assessment of software or hardware that must be incorporated into finished products;
- **Maximise self-assessment through the development and use of harmonised standards**, leveraging the many cybersecurity standards which are already in place, in Europe and globally, to support companies' compliance. An **implementation period of 48 months** should be provided so that the necessary harmonised standards can be delivered, and a bottleneck of third-party assessments avoided;
- When required, **provide for scalable third-party assessments across other legislation, such as the AI Act, and prioritise mutual recognition agreements** to facilitate market access in third countries, particularly with the US as part of the ongoing EU-US Cyber Dialogue;[6]
- **Automatically recognise voluntary cybersecurity certification schemes** approved under the Cybersecurity Act as a means for manufacturers to prove compliance,[7] and stipulate a **direct presumption of conformity vis-à-vis the AI Act**'s cybersecurity requirements;[8]
- **Align incident reporting obligations and timelines with NIS2**, requiring an 'early warning' within 24 hours, followed by an incident notification within 72 hours. For vulnerabilities, ENISA should **establish a European catalogue of known exploited vulnerabilities**, which should be reported by manufacturers;

---

[5] Directive (EU) 2022/2555.

[6] https://digital-strategy.ec.europa.eu/en/news/cybersecurity-eu-holds-8th-dialogue-united-states.

[7] Regulation (EU) 2019/881.

[8] COM(2021) 206 final.

- **Directly repeal the Radio Equipment Directive (RED) delegated act on cybersecurity**,[9] which the CRA makes redundant, and provide for a transition period where compliance with either will be possible; and
- **Create a European regulatory sandbox** to support compliance, particularly for SMEs and start-ups, and to contribute to **regulatory learning** for a future revision of the CRA.

[9] Delegated Regulation (EU) 2022/30.

Table of contents

Capturing the right scope

DIGITALEUROPE has urged that the CRA should focus on creating a clearer compliance framework for connected finished products only.[10] As highlighted by our survey of experts, a horizontal approach for connected devices can properly address the deficiencies of traditional product legislation, which was not designed to cover cybersecurity beyond pure physical features, and deliver common baseline cybersecurity across all connected products.[11]

The European Commission has opted for a much broader scope. The proposal's definition of 'product with digital elements' would comprise not only tangible products, but also all types of software (including all standalone software not linked to a tangible product) and all components (both hardware and software).

The final text will have to ensure the CRA does not cover too much too soon. Any expansion of scope beyond finished tangible products must be clear and enforceable. It should, to the fullest extent possible, avoid duplicative work rather than perpetuate a vague compliance picture for companies and authorities alike – exactly the problem the new law should solve in the first place.

Extending the CE mark to software

To date, software has not been a central part of the New Legislative Framework (NLF), which has traditionally covered placement on the market of physical goods and is now being expanded to cybersecurity.

This means that a whole host of large and small software providers will need to cope with a system they are today largely unfamiliar with. Recent estimates put the number of companies developing software in Europe at more than 370,000, employing almost 1.5 million people.[12]

The NLF system itself must grapple with some inherent novelties brought about by software – compared to how hardware is developed and placed on the market – and be adapted so that it can achieve a good level of effectiveness whilst keeping true to its nature. The same applies to market surveillance authorities and notified bodies, whose expertise has traditionally not encompassed software and cybersecurity.

The difficulties in such adaptation should not be underestimated, lest compliance efforts be made ineffectual.

---

[10] DIGITALEUROPE, *Building blocks for a scalable Cyber Resilience Act*.

[11] DIGITALEUROPE, *Setting the standard: How to secure the Internet of Things*.

[12] IBISWorld, *Software Development in the EU -– Market Research Report*, March 2022.

Standalone software

These considerations are particularly relevant for standalone software.

At present, software separate from products is only envisaged in the medical device regulations,[13] but only to the extent it is specifically intended for one or more regulated medical purposes. General-purpose software is explicitly excluded. Other NLF legislation refers to software only to the extent it is integrated into a tangible product.[14] The CRA would be the first law to cover any software regardless of intended purpose and execution environment.

The need to adapt existing NLF concepts to accommodate software has been one of the central preoccupations of the European Commission's evaluation of the NLF, which was published shortly after the CRA proposal.[15]

Long-standing basic concepts such as placing and making available on the market, affixing the CE mark, or withdrawing or recalling from the market need to be further specified in relation to software in order to avoid inconsistencies and misinterpretation. Similarly, the existing concepts of manufacturer, importer and distributor should be able to incorporate new, non-hardware players in the value chain.

The CRA proposal deals with these topics only in part. The definition of 'manufacturer' (Art. 3(18)) now incorporates software developers, but the specificities of software development and deployment are otherwise largely ignored throughout the proposal, which abides by conventional NLF language.

A further, specific problem is the concept of 'substantial modification' (Art. 3(31)), which must ensure that software updates are not unduly understood as requiring a new conformity assessment or as extending the reference point for compliance.[16] The new Blue Guide on the NLF has expanded on this notion specifically for software, stipulating that updates should in principle 'be assimilated to maintenance operations' unless they modify the software's 'original intended functions, type or performance,' or change the 'nature of the

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

[14] This includes the Machinery Directive (Directive 2006/42/EC) and proposed Regulation (COM(2021) 202 final) as well as the Radio Equipment Directive (Directive 2014/53/EU).

[15] SWD(2022) 364 final.

[16] One example of uncertainty around this concept when it comes to software stems from Art. 10(6), which requires the provision of security updates during the 'expected product lifetime or for a period of five years from the placing of the product on the market.' In the case of software, new versions are regularly released, and the concept of 'expected lifetime' is generally not applicable. It would be illogical to require each version to be supported for five years, long after it has been superseded by multiple new and more secure versions. Continued support of legacy versions provides a disincentive for users to migrate, which the CRA should instead encourage.

hazard' or the 'level of risk.'[17] Such language, however, remains highly ambiguous, with the potential to capture any new features.

Whilst further clarity may be provided in a future overall review of the NLF, we believe that the CRA itself, as the main horizontal law governing software to date, should aim for as much certainty as possible in the legal text itself. Additionally, it should introduce **an obligation for the European Commission to develop guidelines specifying the application of relevant concepts to software**, building on work previously conducted for medical devices.[18] Such guidelines should be developed with input of the Stakeholder Expert Group we suggest creating,[19] as well as through a broader process of open public consultation, and be revised regularly based on learnings from sandboxing.[20]

Moreover, a scalable conformity assessment system – including full availability of harmonised standards for self-assessment whenever applicable, as well as a realistic implementation timeline – will be necessary to cover standalone software effectively.[21]

Remote data processing

The inclusion of 'remote data processing' in the proposal's scope is at odds with Recital 9's intention to exclude software as a service (SaaS), the latter already being regulated under NIS2.[22]

Virtually all software nowadays has forms of data processing at a distance that are essential to it, be they 'designed and developed by the manufacturer or under [its] responsibility.'[23] For example, the Météo-France weather app is merely a software client connecting to the same servers a web browser connects to when visiting the meteofrance.com website. Most apps have similar cloud backends of numerous networked servers, which may consist of SaaS, platform-as-a-service (PaaS) or infrastructure-as-a-service (IaaS) offerings.

---

[17] Pp. 18–19, 2022/C 247/01.

[18] The medical device regulations themselves do not clarify these concepts in the legal text but leave their clarification to interpretative guidance. See MDCG 2019-11.

[19] See 'Amending and specifying the scope' section below.

[20] See 'Sandboxing and review' section below.

[21] See 'Conformity assessment' and 'Application' sections below.

[22] The CRA's explanatory memorandum states (pp. 2-3) that NIS2 ensures 'that technical specifications and measures similar to the essential cybersecurity requirements of the Cyber Resilience Act are also implemented for the design, development and vulnerability handling of software provided as a service (Software-as-a-Service).'

[23] Art. 3(2) of the proposal.

The proposal creates a situation where the same cloud offering may *de facto* be subject both to the CRA as a product with digital elements and to NIS2 as a cloud service provided by an essential or important entity.

In order to circumscribe this inherent overlap, absent a full deletion of remote data processing from the scope, the definition in Art. 3(2) should **exclude the hardware, software and services used for remote data processing, transmission and storage**. This will ensure that at least IaaS and PaaS are not inadvertently included, and reflect Recital 9's intent in an operative provision to the effect that services in and of themselves are out of scope.[24]

Whilst this approach can help to reduce overlap with NIS2, it cannot fully resolve all challenges related to the intersection between SaaS and the notion of remote data processing. We urge that this issue should be further detailed in the above-mentioned guidelines on software, with input from the suggested Stakeholder Expert Group.

Components

NLF legislation typically applies to finished products, with components, spare parts or sub-assemblies only rarely regarded as finished products. Components' end-use necessarily consists of their assembly or incorporation into finished products, whose manufacturers are ultimately responsible for compliance of the complete product.

The CRA proposal contradicts this approach by incorporating all software and hardware components directly into the Art. 3(2) definition of 'product with digital elements,' which refers to 'software or hardware components to be placed on the market separately.'

As we have argued above, this definition is already very broad, comprising not only hardware but also all types of software irrespective of an intended purpose. Additionally, the direct inclusion of components does not take into account that their security largely depends on the products they are to be integrated in, and often cannot be tested meaningfully without the containing product.

Partly completed products

[24] This will also ensure that changes in infrastructure services do not require a new conformity assessment for products with digital elements when the infrastructure boundaries are commercially accessible, either through standardised interfaces or clearly documented integration points. We also note the inclusion of 'hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments' in Class II of Annex III. However, IaaS provides virtual machine environments that are separated from each other precisely by hypervisors or container runtime systems. This might unintentionally bring IaaS into scope.

As seen above, components are usually not explicitly addressed in NLF legislation unless they themselves fall in scope and are placed on the market as such. At such time, they become a finished product in their own right.

However, NLF legislation can be more specific with regard to components and apply special rules to them. The main reason to do so is that a component usually cannot be assessed for its conformity independently. This issue would be even more prominent in the CRA, as components may not mitigate cyber risks, e.g. a RAM chip cannot encrypt its own data, or be tested, e.g. a microprocessor does not run without a motherboard, without being incorporated into a containing product.

To cover this, the part of the Art. 3(2) definition referring to 'software or hardware components to be placed on the market separately' should be removed.[25] Instead, building on the approach already taken in the Machinery Directive and proposed Regulation,[26] the CRA should **introduce the concept of 'partly completed product with digital elements,'** defined as 'a product which cannot function in itself and which is only intended to be incorporated into other products, thereby forming a product with digital elements.' Chapter III should subsequently introduce a dedicated conformity assessment procedure for placement on the market of partly completed products.[27]

This well-tested approach enables manufacturers of partly completed products to identify essential requirements which, given the partial nature of their products, cannot yet be addressed in their own conformity assessment but need to be assessed at a later stage.[28]

To this end, Annex V should include a separate section stipulating 'relevant technical documentation for partly completed products with digital elements,' requiring manufacturers to **specify the essential requirements that are already covered by their partly completed products and those that are**

[25] We note that, precisely because of the broad definition of 'product with digital elements,' most products would fall in scope as such under Art. 3(2) without any reference to components. This is particularly the case given the broad inclusion of all standalone software in the scope. The reference to components in the Art. 3(2) definition is therefore unnecessary at best.

[26] See the definitions of 'partly completed machinery' at Arts 2(g) of the Machinery Directive and 3(10) of the proposed Regulation.

[27] See Arts 13 of the current Machinery Directive and 22 of the proposed Regulation. Although not requiring the CE mark, this procedure would allow partly completed products to be placed on the market.

[28] This approach is especially valuable for hardware products, whilst it might be less applicable to software, notably standalone software. Because of the broad definition of 'product with digital elements,' software is more likely to be in scope as a product as such, with flexibility in the application of the Annex I essential requirements being particularly important ('where applicable,' as we highlight in the 'Obligations and essential requirements' section below). This could also be addressed in the proposed guidelines on software.

not. A separate annex should provide for a **'declaration of incorporation'** in lieu of the declaration of conformity for partly completed products.[29]

General-purpose microprocessors

Annex III identifies some specific components as being directly in scope. Importantly, this includes general-purpose microprocessors, whose capabilities to comply with the CRA's essential requirements are limited without considering their integration into, and the operational environment of, the finished product. Considering the various contexts and risk environments where general-purpose microprocessors may be utilised, as well as essential interoperability considerations, many evaluations are more appropriately done at the final stage of product go-to-market.

Because of this – and because of their nature as mass products, for which mandatory third-party assessment would be exceedingly cumbersome – **general-purpose microprocessors should be moved from Class II to Class I of Annex III**.

This will allow for a more streamlined compliance process of such general-purpose components, based on harmonised standards as opposed to third-party conformity assessment, whilst still allowing for the necessary further due diligence at the finished product stage pursuant to Art. 10(4). This will be particularly important in order not to compound the current semiconductor shortage with new conformity assessment bottlenecks.

Further exclusions

The inclusion of remote data processing in the definition of product with digital elements could also be misinterpreted to include websites. This is because websites often send software such as JavaScript code to users' browsers for execution, for example to provide for rich and dynamic content. Such **website software should be clearly carved out of the CRA's scope** so there is no ambiguity about portions of websites being in scope.

We welcome the acknowledgment at Recital 21 and Art. 4(3) that modern software development requires the release of **'unfinished software'** for feedback, testing and bug discovery (also known as 'alpha' and 'beta' releases), and that such software should not be in scope. Importantly, individuals who sign up to be alpha/beta users are sophisticated technology consumers, who understand the software is incomplete and simply want to experience the latest features and steer the product's direction with their feedback.

[29] This mirrors Annexes VI(B) of the current Machinery Directive and IV(B) of the proposed Regulation, and Annexes II(1)(B) of the current Directive and V of the proposed Regulation, respectively.

Similarly, we welcome the **exclusion of open-source software** (OSS) at Recital 10, and urge such exclusion should be reflected in Art. 2. However, the recital's broad interpretation of 'commercial activity' does not accurately reflect operational best practices, governance and licensing in an OSS context. A goal-oriented exception in favour of upstream OSS research and innovation should support all activities in which users receive all rights to the OSS, and with which the users are supported in exercising such rights. Technical support services can be critical to this end, and should therefore not be considered as a commercial activity.

We suggest excluding from Art. 2's scope **items that are 'inherently benign,'** that is, which by their nature do not have an impact on the security of the intended operational environment, such as the above-mentioned RAM chips. This reflects the approach already taken in the Electromagnetic Compatibility Directive,[30] as well as in the Low Voltage Directive.[31]

Consistent with most NLF legislation,[32] and necessary to allow for reparability of hardware products, Art. 2 should also make it explicit that the CRA does not apply to **spare parts** intended to replace identical components.

Finally, we suggest clarifying that **products exclusively produced, supplied and used within the same corporate group**, and not made available on the internal market outside of that group, are excluded.

Amending and specifying the scope

Proposed Arts 6(2) and (3) would allow the Commission to adopt delegated acts to amend the list of critical products contained in Annex III and to specify the definitions in Annex III.

Whilst a mechanism to update the list of critical products may be necessary, we believe that the CRA's initial scope should be clearly stated in the final text itself, and that **Art. 6(3) should therefore be deleted**.

A protracted period of uncertainty as the Commission stipulates new elements that may well change the text's material scope would be greatly damaging to the development of harmonised standards and to manufacturers' compliance efforts. It is particularly troubling that this substantial power is provided with no adjustment to the CRA's entry into force, which based on the proposal may

[30] See Recital 12, Directive 2014/30/EU.

[31] The 2018 Guide to Directive 2014/35/EU stipulates that 'some types of electrical devices, designed and manufactured for being used as basic components to be incorporated into other electrical equipment, are such that their safety to a very large extent depends on how they are integrated into the final product and the overall characteristics of the final product. … [S]uch basic components, the safety of which can only, to a very large extent, be assessed taking into account how they are incorporated and for which a risk assessment cannot be undertaken, … are not covered as such by the LVD. In particular, they must not be CE marked unless covered by other Union legislation that requires CE marking.'

[32] See, for example, Art. 1(2)(a) of the Machinery Directive.

occur a mere 12 months after the Commission's 'specification' of the CRA's scope.

Chapter VI should establish, in addition to the national experts assisting the Commission and open public consultations, **a Stakeholder Expert Group to advise the Commission on the exercise of its powers** – including, crucially, Art. 6(2) delegated acts.[33] The need for a non-binding Opinion from this group should be reflected in Arts 50-51.

Conformity assessment

Workable conformity assessment processes will be pivotal to the CRA's practical implementation and success. Once more, this is particularly the case due to the CRA's very broad scope, which must make it practical for a broad array of companies to comply with its requirements.

We strongly welcome the European Commission's decision to closely adhere to the NLF on this very important aspect. The use of conformity assessment modules offers a risk-based approach consistent with the NLF.

Central role of harmonised standards

The NLF sees the existence of harmonised standards as a vital route for manufacturers to prove their compliance. This is reflected in the CRA proposal, which under Module A allows manufacturers to perform internal controls based on harmonised standards and only mandates more cumbersome third-party assessments under Modules B, C and H for products classified as critical (Class II of Annex III).[34]

What are harmonised standards?

Harmonised standards are standards developed by recognised European standardisation organisations (ESOs: CEN, CENELEC or ETSI) following a request from the European Commission. Such request provides the conditions that the requested standard must respect to meet the legal requirements or other provisions set out in relevant EU legislation. Subject to verification by the Commission that these conditions have been met, a reference to the standard is subsequently published in the Official Journal of the European Union (OJEU).

Harmonised standards lay down the technical specifications necessary for products to meet the essential legal requirements under relevant EU product legislation. By doing so, harmonised standards are the technical foundation to ensure legal conformity in a uniform way across all the EU, supporting the free movement of goods in the EU single market. Their existence also simplifies the tasks of market surveillance authorities, which ensure safety of all products across Europe.

[33] We note, in passing, that Art. 6(2)(c) mentions the 'processing of personal data' as a 'critical or sensitive function' that may justify incorporation in the list of critical products. The processing of personal data is so widespread that its mention, even as a non-exhaustive example, is moot. We suggest it should be deleted.

[34] Art. 24 of the proposal. The different modules are described in the proposal's Annex VI.

Manufacturing products in accordance with harmonised standards implies they are in conformity with the corresponding legal requirements. This allows manufacturers to place their products on the market under a swifter procedure.[35]

The use of harmonised standards is voluntary. However, if a harmonised standard is not available, compliance with legal requirements must be proved using other conformity assessment procedures. In most cases, this will require an assessment by 'notified bodies,' third parties officially designated by national authorities to carry out such tasks.

It has been estimated that third-party assessment can cost up to €40,000 per product,[36] which is challenging especially for smaller companies and for less expensive products.

There already exist a number of standards that cater to most of the essential requirements laid out in the CRA, and which should be leveraged for the creation of harmonised standards to prove compliance with it. In addition to the standards being developed pursuant to the RED delegated act on cybersecurity,[37] such standards include:

- The widely used ISO/IEC 27001 (information security management);
- ISO/IEC 27002 (information security controls);
- Draft ISO/IEC 27402 (DIS) (IoT device baseline requirements), soon to be finalised;
- ETSI EN 303 645 (IoT consumer products);
- ETSI TS 103 732 (consumer mobile device);
- ETSI TS 103 848 (home gateway products);
- The EN IEC 62443 series of standards for electronically secure industrial automation and control systems (IACS);
- ISO/IEC 29147 and 30111 (vulnerability disclosure and handling);
- The ISO/IEC 27036 series for supply chain security;
- ISO/IEC 27034 (application security);
- The Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408);

[35] More detailed information about harmonised standards can be found in Section 4.1.2 of the European Commission's *Blue Guide* on the implementation of EU products rules, 2022/C 247/01.

[36] *Commission Staff Working Document Part 1: Evaluation of the Internal Market Legislation for Industrial Products*, available at https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52014SC0023

[37] On the relationship with the RED delegated act, see 'Radio Equipment Directive' section below.

- ISO/IEC 27033 (network security) and ISO/IEC 27035 (information security incident management); and
- The Cybersecurity Framework, the Secure Software Development Framework, and the Security and Privacy Controls for Information Systems and Organisations developed by the US National Institute of Standards and Technology (NIST).

The Commission's standardisation requests for CRA harmonised standards should therefore allow ESOs to develop harmonised standards based largely, if not exclusively, on existing standardisation work. This will ensure timely availability of harmonised standards and much more effective compliance by manufacturers.

By contrast, standardisation requests deviating from existing standards would require additional standards development work, which would result in delays and the potential unavailability of harmonised standards by the time the CRA comes into application.

Common specifications

The power for the Commission to unilaterally write common specifications, if harmonised standards are unavailable or if it deems they are 'insufficient' or subject to 'undue delays,'[38] is harmful to the healthy development of harmonised standards.

ESOs should be empowered to develop harmonised standards via standardisation requests that allow adequate time to ensure that high-quality standards can be produced through multistakeholder expert engagement. Common specifications bypass such established standardisation processes, and disrupt efforts to develop consensus-based, market-driven, fair, inclusive and transparent standards.

Any disincentives to make full use of harmonised standards must be avoided, particularly considering the already ample power the Commission enjoys throughout the harmonised standardisation process. The Commission not only adopts requirements that are mandatory for ESOs' development of harmonised standards, but has the ultimate authority to ratify whether these requirements have been met. ESOs, on the other hand, have all the necessary incentives to engage in good-faith efforts to complete standardisation requests in time, given that failure to do so would result in the unavailability of harmonised standards and force manufacturers to engage in expensive third-party assessments instead.

Art. 19 and all related references to common specifications should therefore be deleted.

[38] Art. 19 of the CRA proposal.

Scalable third-party assessment

The CRA relies on the NLF's Modules B, C and H, involving third-party assessment as opposed to self-assessment by the manufacturer, where harmonised standards are not available (especially for Class I critical products), where third-party assessments are mandatory (for Class II critical products), or indeed where manufacturers themselves opt for notified bodies instead of internal controls.

This approach is welcome. At the same time, scalability of such third-party assessments will have to be ensured due to the CRA's not insignificant list of critical products, the growing body of other NLF legislation that may require third-party assessments, and the existence of relevant quality management certifications predating the CRA.

For **Module B**, the **requirement for notified bodies to assess 'specimens** of one or more critical parts' **should be deleted**. Such additional testing is not requested under the RED, nor is it required under more recent NLF-based proposals such as the AI Act. Testing by the manufacturer or by test laboratories on the manufacturer's behalf is sufficient, whilst additional testing by notified bodies would overburden the process, with no benefits compared to a more effective system based on products' technical documentation and supporting evidence.

Module H has potential to streamline third-party conformity assessments, not only under the CRA but also under other NLF legislation that may apply to the same products, such as the proposed AI Act.

Unlike the combination of Modules B and C, Module H does not require examination of each individual product in scope from any given manufacturer, but instead allows manufacturers to ensure compliance by having their quality assurance system assessed by a notified body, thus covering all relevant products.

This remains a costly and demanding process, and has been used sparingly thus far. However, the CRA's broad scope might make it a more appealing option.

In addition, **Module H should be recognised as a basis for manufacturers' compliance not only with the CRA, but with multiple NLF-based legal acts**. This should be explicitly provided for in Art. 24, as well as in Art. 43 of the proposed AI Act.

Mutual recognition

Finally, it must be considered that there already exist several certifications for information security management, which in most cases will apply beyond the EU, such as those based on ISO/IEC 27001 and related standards, that companies may already have in place. By the same token, conformity

assessment bodies will need to be ready to scale internationally, including to tackle the skills shortage generated by increasing demand for cybersecurity professionals.

This underlines again the importance of aligning the CRA's essential requirements and harmonised standards with existing cybersecurity standards, as well as of quickly strengthening mutual recognition agreements (MRAs) with third countries.

MRAs allow for non-EU countries to accept conformity assessments performed by EU-designated notified bodies, and conversely for the EU to accept conformity assessments performed in third countries.

At present, for example, MRAs are in place with Japan and the US but cover a limited number of products.[39] Given the growing role of NLF legislation being written in the EU, as well as cybersecurity requirements being introduced in other geographies,[40] expanding these agreements becomes a matter of priority in order to avoid wasteful fragmentation.

The CRA proposal recognises this at Recital 67, whilst unfortunately the AI Act proposal does not include any mentions of mutual recognition. We strongly encourage co-legislators to **introduce an explicit mandate for the European Commission to conclude and update MRAs with third countries** in order to facilitate market access. This could be done at the end of Chapters III or IV.

We urge, in particular, the US administration and the European Commission to make MRAs a priority in future iterations of the EU-US Cyber Dialogue.

Cybersecurity certification schemes

Proposed Art. 6(4) institutes a process whereby the Commission can identify, through implementing acts, a new category of 'highly critical products with digital elements' for which certification pursuant to the Cybersecurity Act, as opposed to the NLF modules, is made mandatory.

The creation of a 'highly critical' category that does not follow the NLF should be rejected. The Commission is already empowered to amend the lists of critical products, including those that should undergo third-party conformity assessment, under Art. 6(2). If a product is in the future considered 'highly critical,' it should simply be included anew under Class II of Annex III to ensure a heightened level of conformity assessment.

In addition, the criteria for specifying 'highly critical products' requiring mandatory certification overlap considerably with considerations regarding the

[39] https://single-market-economy.ec.europa.eu/single-market/goods/international-aspects-single-market/mutual-recognition-agreements_en.

[40] See, in particular, the May 2021 EO 14028 in the US, which among other things directs NIST to initiate two labelling programmes on software development practices and IoT cybersecurity.

use of critical products by essential entities covered by NIS2. The Commission is already empowered to adopt delegated acts under Art. 24 NIS2 to require essential or important entities to use only certified products, services or processes.[41]

At the same time, the role of cybersecurity certification schemes in ensuring CRA compliance should be larger than envisaged in the proposal.

Arts 18(3) and (4) currently limit the role of schemes to instances where the Commission has adopted implementing acts granting that an approved scheme may be used for CRA conformity, including whether such scheme obviates the need for third-party assessment.

DIGITALEUROPE believes that the CRA should establish a much more straightforward and pragmatic route for manufacturers to rely on schemes, should they wish to pursue certification rather than follow one of the NLF modules.

The Cybersecurity Act is not only an official EU legal act, but one which sets out comprehensive security objectives and a rigorous process for the creation and approval of schemes, overseen by the European Commission itself and ENISA. It is perplexing that it should only be presumed to ensure compliance with essential cybersecurity requirements only when its adequacy is reassessed and sanctioned in a separate act.

Art. 18(4) requiring a separate implementing act to recognise EU cybersecurity certification schemes should be deleted, as should relevant references such as that at Art. 18(3). Products certified pursuant to the Cybersecurity Act should automatically be presumed to be in conformity with the CRA's essential requirements.

Manufacturers should be free to choose whether to follow one of the NLF modules or whether to **voluntarily pursue cybersecurity certification as a means to prove compliance**.[42]

Obligations and essential requirements

[41] Art. 6(4) of the proposal is therefore superfluous at best. In addition, it bypasses the important impact assessment required of the Commission by Art. 56 of the Cybersecurity Act before schemes can be mandated, which is referenced by Art. 24(2) NIS2.

[42] We note that the proposal to require an implementing act may have been driven by potential conflicts with mandatory third-party certification required for critical products under Class II of Annex III, as well as by concerns that certification schemes may not meet the CRA's essential requirements. However, we note that no schemes have been adopted to date, and that the only scheme about to be finalised (the EUCC scheme) does not include a self-assessment option. More broadly, alignment with the CRA's essential requirements, assurance levels and assessments will necessarily need to be factored in to any ongoing draft schemes now that the CRA has been proposed. We also note that the CRA should provide baseline requirements, cybersecurity schemes being able to go beyond them to achieve higher assurance.

Annex I and Art. 10 delineate obligations for economic operators and essential requirements that are largely in line with industry best practice. Furthermore, we welcome the recognition that essential requirements should apply 'where applicable,'[43] which will allow product specificities to be taken into account based on a risk assessment.

As argued above, such flexibility is vital given the proposal's broad scope. Appropriate cybersecurity measures may differ from product to product, including in terms of what can be considered commercially reasonable, for example in a consumer versus a business-to-business (B2B) context.[44]

Some of the obligations and requirements, however, should be scoped down.

Aligning reporting to NIS2

The proposal's Arts 11(1) and (2) set out reporting obligations pertaining to 'actively exploited vulnerabilities' and to 'incident[s] having impact on the security' of products. The deadline to report both is set at 24 hours.

Reporting obligations were just recently heavily debated as part of the **NIS2** negotiations.[45] We urge that the results of these difficult negotiations should be **swiftly replicated in the CRA**. This will guarantee alignment and predictability of both obligations and outcomes, also considering that companies' teams responsible for responding to security incidents will tend to be the same for entities covered by both laws.

Incidents

Art. 11(2)'s **obligation to notify incidents should be circumscribed to incidents having a *significant* impact** on products' security, reflecting the language in Art. 23(1) NIS2 ('significant incident').[46]

A clear distinction should be drawn between significant incidents and vulnerabilities, 'incidents' being usually equated with 'vulnerabilities' from a product security perspective. Similar to NIS2,[47] the CRA should introduce **thresholds** to establish when an incident can be considered significant. These

[43] Section 1(3), Annex I of the CRA proposal.

[44] One example is the secure-by-default configuration requirement in Annex I(1)(3)(a). Whilst this may make sense in a consumer environment, the most secure configuration in an enterprise setting is highly dependent on contextual factors such as the configuration and versions of interconnected devices and networks. Another example is the potential trade-off between different essential requirements. Minimising the attack surface may come at the cost of making software updateable, such as by making firmware read-only.

[45] See NIS2's Art. 23.

[46] It must be added that Art. 30 NIS2 allows voluntary notification of information other than notification of significant incidents (other incidents, cyber threats and near misses), including by entities not subject to NIS2. A similar provision could be introduced in the CRA.

[47] Art. 23(3), ibid.

should refer to parameters reflecting malicious behaviour that could genuinely compromise the product or user, such as that the incident could result in material harm to the user.

Unlike proposed Art. 11(4), which obliges manufacturers to notify users about all incidents, the final CRA text should align to NIS2 by requiring, 'where appropriate,' notification to users of 'significant incidents that are likely to adversely affect' a product's security.[48]

Incident reporting timelines should be aligned to those set out in Art. 23(4) NIS2, requiring only an **'early warning' within 24 hours**, followed by an **incident notification within 72 hours**. Like NIS2, the final CRA text should specify that the mere act of notification shall not subject manufacturers to increased liability.

As heavily debated for NIS2, a 24-hour notification deadline would ignore the complexity of investigating and remediating cyber-attacks, resulting in excessive reporting based on insufficient or unreliable information that would render reports largely meaningless. Just as important to generate reliable information is the point at which the manufacturer is deemed to be 'aware' of an incident, which should be no sooner than when the incident has been triaged by the appropriate incident response team.[49]

Finally, the CRA should provide that reporting of significant incidents to ENISA pursuant to the CRA should subsume equivalent reporting obligations under Art. 23 NIS2, with ENISA informing, as currently envisaged, the relevant single points of contact and, if relevant, the European cyber crisis liaison organisation network (EU-CyCLONe). Single points of contact should in turn be required to inform CSIRTs or, where applicable, the competent authority under NIS2.

Vulnerabilities

Mandatory reporting of 'actively exploited vulnerabilities' should be excluded.

Whilst certain disclosures may be necessary, especially when products are deployed in B2B contexts to allow mitigation measures, premature reporting of unpatched vulnerabilities across the board will create considerable new cybersecurity risks, in addition to deviating from established standards for coordinated vulnerability disclosure.[50] Similar obligations introduced in other

[48] Art. 23(1), ibid. This would capture, for example, incidents that impact the integrity or confidentiality of the source code of software during the design and development phase, which are a source of supply chain attacks such as SolarWinds.

[49] This is in line with best practice for personal data breach notifications under the GDPR, as reflected at para. 34 of draft EDPB Guidelines 9/2022, revising WP250 rev.01.

[50] ISO/IEC 29147 referenced above, for example, requires disclosure only after the development and deployment of remediation.

jurisdictions are likely to have resulted in increased exploitation of zero-day vulnerabilities this past year.[51]

Instead, as with 'cyber threats' under NIS2,[52] manufacturers should **'where appropriate' communicate to potentially affected users any measures or remedies they can take** in response to a significant vulnerability. As stated above, this is particularly important to allow for mitigation measures in a B2B context.

In addition, complementing the European vulnerability database created by Art. 12(2) NIS2, **ENISA should be tasked with establishing and maintaining a European catalogue of known exploited vulnerabilities** which can be patched. Manufacturers should be required to report instances where their products contain vulnerabilities included in such catalogue.

This catalogue would build a picture of the landscape of high-risk vulnerabilities to be mitigated from a product perspective, and act as a central source of information about which of the many thousands of existing vulnerabilities are highest risk in practice and should be prioritised.[53]

Finally, Annex I(1)(2) requires products to be 'delivered' without any known exploitable vulnerabilities. Whilst we agree that vulnerabilities should as much as possible be avoided, an approach based on risk should be adopted in this respect.

Certain vulnerabilities may present negligible risks that will not result in incidents. It will be unnecessary and burdensome for a manufacturer to be forced to fix any issue, no matter how small and no matter the cost. The mere existence of a vulnerability should not in itself block a product from, or force it off, the market. This would otherwise result in the mass unavailability or removal of essentially secure products.

A more proportionate approach would be to **require manufacturers to document instances of vulnerabilities in their products that are not significant** at the time of placing on the market, and why they have reached such assessment.

In addition, products are often designed for years or sit in storage for months before being turned on and updated. By that time, new vulnerabilities that were not known during or before the manufacturing process could have developed.

[51] See p. 39, *Microsoft Digital Defense Report 2022*, available at https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022.

[52] Art. 23(2), ibid.

[53] Most vulnerabilities in products are from third-party components, and the biggest job is getting companies to act on vulnerabilities that present a significant risk. As of November 2022, 21,600 new vulnerabilities were recorded in NIST's National Vulnerability Database in 2022, and the total number of listed common vulnerabilities and exposures (CVEs) is about to cross the 200,000 mark. This approach has already been adopted in the US with CISA's Known Exploited Vulnerability Catalog, and we urge ENISA to coordinate closely with CISA in the establishment and maintenance of its own catalogue.

The time of delivery is hence irrelevant – what matters is the time of deployment and subsequent installation of updates.

For this reason, the proposed requirements for **vulnerabilities to be addressed through security updates**, with instructions and features being provided to install updates as products are provisioned,[54] should be referred to in Annex I(1)(2) and be considered as sufficient.

Software bill of materials

Annex I(2)(1) sets out an obligation to draw up a software bill of materials (SBOM) 'in a commonly used and machine-readable format.' Art. 10(15) gives the Commission the power to adopt implementing acts specifying the related format and elements.

This appears to have been inspired by ongoing efforts in the US, where the May 2021 EO 14028 has mandated SBOMs for products purchased by federal departments and agencies.

SBOMs can be very large and complex, and multiple formats in different jurisdictions will be burdensome to comply with for manufacturers. In addition, SBOMs are still a relatively nascent concept, and clearly established formats and elements are still lacking.[55]

In light of the incipient nature of SBOMs, we urge that at this stage they should be **based on guidelines to be developed by the Commission, rather than binding implementing acts**. We also urge the Commission and the US administration to include SBOMs in future iterations of the EU-US Cyber Dialogue.

Moreover, Annex I(2)(1) appears to include the disclosure of vulnerabilities within SBOMs. Combined with Annex II(6)'s requirement to make SBOMs available to users, this would be extremely counterproductive.[56]

Making vulnerabilities public information, especially if unpatched, would offer cyber criminals easy access to cause cybersecurity incidents, particularly if such information is provided in machine-readable formats that could allow them to automate the detection of attack surfaces. Indeed, this applies more broadly to SBOMs in general, public availability of which may make it easier for attackers to pursue their goals.

---

[54] See the proposal's Annex I(1)(3)(k), Annex I(2)(2) and Annex II(9)(c).

[55] The US National Telecommunications and Information Administration (NTIA) has published guidance on minimum SBOM elements, available at https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf, which acknowledges that SBOM capabilities are currently nascent for federal acquirers and that the minimum elements are but 'a key, initial step in the SBOM process that will advance and mature over time.'

[56] NTIA guidance (p. 17) recommends 'that vulnerability data be tracked in separate data structures from the SBOM.'

For this reason, the **reference to vulnerabilities in Annex I(2)(1) should be deleted, and Annex II(6) should be changed to clarify that SBOMs are not to be made publicly accessible**.

SBOMs should be made available to notified bodies and market surveillance authorities for the exercise of their tasks and under the strict non-disclosure conditions set out in Art. 52.

Relationship with other legal acts

In addition to its relationship with certification schemes pursuant to the Cybersecurity Act, the final CRA text should also more clearly establish its relationship with other applicable EU legislation.

Radio Equipment Directive

We are particularly concerned that the proposed CRA does not outright establish its relationship with the RED.[57] The RED delegated act to ensure network protection, the protection of personal data and privacy, and protection from fraud is in essence a precursor to the CRA's cybersecurity requirements.

The Commission's proposal only includes a mention in the explanatory memorandum and at Recital 15, explaining that, although 'the essential requirements laid down in [the CRA] are aligned with the objectives of the requirements for specific standards included' in the RED delegated act's standardisation request, the Commission reserves itself the prerogative to decide '*if* [it] repeals *or amends*' (emphasis added) such delegated act.

Given that the CRA will cover all products covered by the RED, and that its essential requirements go beyond those contained in the delegated act, the CRA itself under Chapter VIII should **directly repeal the RED delegated act and establish a transition period where compliance with either legal act would automatically provide presumption of conformity with the other**.[58]

Furthermore, whilst Recital 15 promises that the Commission should 'take into account' the standardisation work carried out pursuant to the RED delegates

[57] Directive 2014/53/EU.

[58] It has been argued that an EU legal act cannot repeal a delegated act adopted pursuant to another EU legal act. This claim, however, runs counter to basic rules regarding the relationship between legal acts or past experience where delegated acts adopted under one EU legal act amended delegated acts adopted under other EU legal acts. One such example is the horizontal Commission Regulation (EC) No 1275/2008 on ecodesign requirements for standby and off-mode electric power consumption, which overlapped with the vertical Commission Regulation (EC) No 278/2009 on ecodesign requirements for no-load condition electric power consumption and average active efficiency of external power supplies. Art. 8 of Regulation (EC) No 278/2009 amended the earlier horizontal act to exclude certain products which were in its scope. This prevented both acts unnecessarily applying to the same product. This situation maps perfectly the legal process allowing the later CRA to include text to repeal (as there is no possibility to scope out) the earlier RED delegated act and prevent unnecessary overlap of requirements.

act's standardisation request, we urge that this should be reflected in an operative provision under Chapter VIII.

AI Act

Art. 8 should demarcate a clearer relationship between the CRA and the cybersecurity requirements in Art. 15 of the AI Act proposal, similar to what is done with respect to the Machinery Regulation under Art. 9.

Art. 42(2) of the AI Act proposal provides for a clear-cut presumption of conformity with its cybersecurity requirements for high-risk AI systems which have been certified under an approved Cybersecurity Act scheme. The same **direct presumption of conformity** should be in place **for high-risk AI systems falling within the CRA's scope**.

This can be achieved by **retaining and simplifying Art. 8(1) and deleting Arts 8(2) and (3)**. There should be no confusion as to the relevant conformity assessment procedure to be followed, which should be that required under the CRA.

Market surveillance

DIGITALEUROPE appreciates the CRA's explicit reference to Regulation 2019/1020, which ensures stringent surveillance and enforcement of product legislation. Only if conformity assessment – regardless of whether by manufacturers or third parties – is accompanied by effective market surveillance can customers and businesses rely on sufficient cyber resilience.

For market surveillance to be effective when it comes to cybersecurity, the **necessary competences need to be built up**. Although IT cybersecurity as such is a known domain, the CRA requires knowhow in product security, which differs from general IT security. On the other hand, the important role that processes play in cybersecurity goes beyond the traditional product-based expertise of market surveillance authorities.

The key challenge will be the **availability of skilled personnel**. There will be competition between notified bodies, national authorities and companies, who all need the same kind of experts. The requirement in Art. 41(6) for Member States to provide adequate resources must be read and is particularly important in this context.

We welcome proportionality being a central tenet of Chapter V on enforcement. Any actions of Member State authorities must always start on reasoned and justified grounds. From this perspective, although mirroring other NLF legislation, Art. 46 can lead to the withdrawal of compliant products that may be deemed to present not only significant cybersecurity, health or safety risks, but also compliance risks in relation to fundamental rights or 'other aspects of public interest protection.' This **list appears to be overly broad and vague, and should be restricted to significant cybersecurity risks and to health**

or safety risks, in line with the proposal's scope. Any risks pertaining to products' use by essential entities should be dealt with under NIS2.

With respect to **penalties** (Art. 53), we suggest that the calculation **should be based on the amount of the turnover which corresponds to the relevant incompliant product**. Also, the margin in connection with the turnover should be considered for the calculation of penalties.

Application

DIGITALEUROPE believes that a transition period of 24 months as suggested in Art. 57 will be too short for several reasons.

Firstly, given the CRA's wide scope, it is likely that many product groups **won't have harmonised standards available**. This is relevant for products for which self-assessment against harmonised standards will be possible, but also for critical products which must undergo third-party assessment. Notified bodies are dependent on harmonised standards, too.

Secondly, as we argue above, both notified bodies and enforcement authorities are **highly unlikely to have sufficient resources available, nor processes in place**, within such timeframe. They need a ramp-up phase to recruit sufficient staff and adapt to new CRA methodologies.

Both aspects are likely to cause a bottleneck with notified bodies, leading to delays of time to market, increased cost and disruption of supply chains. Recently there has been ample evidence of such challenges with the transition period for the medical device regulations, for which the Commission has just proposed a delay of at least three and a half years to fix ongoing issues with product assessments.[59]

For tangible products, platform and architecture decisions are made many years before a product is finally placed on the market. In preparing to place products on the market, manufacturers need clear predictable requirements to plan, design, develop and prepare conformity assessment materials. Such predictable requirements are **only available when the relevant harmonised standards are published** in the OJEU. Alternative approaches such as common specifications or certification schemes would not necessarily be quicker, and might add to manufacturers' confusion and uncertainty if developed in parallel to potential harmonised standards.

In light of the above, we propose that **the implementation period should be extended to 48 months**. This is roughly the time needed to introduce, verify and list harmonised standards in the OJEU, as well as to adapt products accordingly. Whilst some products may meet the requirements beforehand, more time will be needed overall for the system to develop.

[59] COM(2023) 10 final.

Reporting obligations

Art. 57 envisages that Art. 11's reporting obligations would apply within 12 months, that is, before products can be placed on the market pursuant to the whole CRA. Additionally, Art. 53(3) automatically extends reporting obligations to all software and hardware products placed on the market before the CRA's entry into application.

These provisions ignore the inherent compliance link between the CRA's essential requirements and incident/vulnerability handling processes. Making reporting obligations applicable before the rest of the CRA is in place will in essence expose manufacturers to unrealistic, retroactive expectations of compliance they will be unable to meet.

For these reasons, **Art. 53(3) and the part of Art. 57 referring to Art. 11 should be deleted**.

Sandboxing and review

In light of the CRA's broad scope, as well as the specific novelties brought about by software,[60] we urge co-legislators to introduce measures pertaining to regulatory sandboxes in the final text.

The CRA's general expansion of the NLF to cybersecurity and software requires an environment that supports the design, development and production of products with digital elements, particularly to facilitate compliance and reduce regulatory burden for SMEs and start-ups. Moreover, a process of regulatory learning should be introduced with a view to contributing to a more evidence-based evaluation and review of the CRA.

The AI Act, a twin proposal expanding the NLF beyond hardware, introduces regulatory sandboxes to further these goals.[61] We believe that the CRA should build and improve on the AI Act model. In particular, we believe that possible challenges and fragmentation resulting from purely voluntary sandboxes at Member State level should be overcome by a European process.

To this end, Chapter VIII should create an **obligation for the European Commission and ENISA to establish a European regulatory sandbox** for the design, development and production of products with digital elements, under the Commission and ENISA's direct supervision, guidance and support, which companies can voluntarily participate in before their products are placed on the market pursuant to the CRA. In addition to these objectives, the sandbox should explicitly aim to **contribute to evidence-based regulatory learning**.

---

[60] See 'Extending the CE mark to software' section above.

[61] See Art. 53 of the AI Act proposal, particularly the inclusion of 'evidence-based regulatory learning' in the Council's general approach (doc. 15698/22).

To this end, as part of the CRA's evaluation and review, Art. 56 should also include an **obligation for the Commission to submit appropriate proposals to amend the CRA**, if necessary and in particular **taking into account evidence gathered in the European regulatory sandbox** as well as non-binding opinions issued by the Stakeholder Expert Group and the national experts assisting the Commission pursuant to Arts 50-51.

FOR MORE INFORMATION, PLEASE CONTACT:

- Alberto Di Felice
  Director for Infrastructure, Privacy and Security Policy
  alberto.difelice@digitaleurope.org / +32 471 99 34 25
- Zoey Stambolliu
  Senior Manager for Infrastructure and Security Policy
  zoey.stambolliu@digitaleurope.org / +32 498 88 63 05

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, as well as international policies that have an impact on Europe's digital economy. Our membership represents over 45,000 businesses who operate and invest in Europe. It includes 96 corporations which are global leaders in their field of activity, as well as 41 national trade associations from across Europe.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Assent, Autodesk, Banco Santander, Bayer, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, CyberArk, Danfoss, Dassault Systèmes, DATEV, Dell, Eaton, Epson, Ericsson, ESET, EY, Fujitsu, GlaxoSmithKline, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, Intel, Johnson & Johnson, Johnson Controls International, Konica Minolta, Kry, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Meta, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nemetschek, NetApp, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Red Hat, RELX, ResMed, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Skillsoft, Sky CP, Sony, Sopra Steria, Swatch Group, Technicolor, Texas Instruments, TikTok, Toshiba, TP Vision, UnitedHealth Group, Visa, Vivo, VMware, Waymo, Workday, Xerox, Xiaomi, Zoom.

National Trade Associations

Austria: IOÖ
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Czech Republic: AAVIT
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, SECIMAVI, numeum
Germany: bitkom, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: Infobalt
Luxembourg: APSI
Moldova: ATIC
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS
Slovakia: ITAS
Slovenia: ICT Association of Slovenia at CCIS
Spain: Adigital, AMETIC
Sweden: TechSverige, Teknikföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT Ukraine
United Kingdom: techUK