EUROSMART
The Voice of the Digital Security Industry

# Eurosmart's priorities for the Cyber Resilience Act

## Comments on the European Parliament negotiating position and, on the Council General Approach

Eurosmart welcomes the recent achievements of the co-legislators on the Cyber Resilience Act (CRA) to provide more consistency with the already existing EU cybersecurity regulatory landscape.

As an organization dedicated to promoting secure digital interactions and privacy protection for individuals, we believe that the proposals deserve further improvement to adequately fit in with the EU cybersecurity regulatory landscape.

The digital security industry reiterates some concerns that have been already addressed through a previous white paper. The junction between safety and cybersecurity must be clarified, legal definitions and clarification on the CRA requirements for EU cybersecurity certified products should be provided. For obligations to manufacturer including the definition of product lifetime, security update requirements, incident mechanism and disclosure of vulnerability, Eurosmart would like to raise the co-legislator's attention to the mechanism that are already in place for EUCC (today SOG-IS) certified product or products falling under the scope of the NIS2. A full alignment with NIS2 and other requirements that are already in used for this kind of products should be ensured.

Moreover, certification obligation in the CRA context for all high-end security products will complexify existing high-level evaluation processes. Instead of an obligation, Eurosmart recommends working and relying on "presumption of conformity" that could be provided by EU cybersecurity certificates.

Therefore, Eurosmart points out the following provisions:

1. **Required use of European cybersecurity certification schemes**
2. **Common specifications**
3. **High-risk AI system**
4. **Obligations of manufacturer**
   - 4.1. On components
   - 4.2. Product life-time – Support period
   - 4.3. Security update

# 1. Required use of European cybersecurity certification schemes

EU Council
*Article 6a - Also refer to recital (27a) and (27aa)*

European Parliament
*Article 6(5))*

Eurosmart recommends prioritising the implementation of the CRA principles like implementation of Essential cybersecurity requirements on product categories where the conformance mechanisms are not yet regular practice. Certification obligation in the CRA context for all high-end security products will complexify existing high-level evaluation processes. Several types of evaluations are already required for various sectors and have maintained products at the State-of-the-Art for years through the assessment of advanced and sector-specific security requirements.

**Eurosmart invites the co-legislators to reconsider the European Council proposal focusing on certification obligation for all high-end security products.**

**In the meantime, effort should be made to recognised EU cybersecurity certification schemes as a mean to demonstrate conformity with the CRA essential requirements. In this respect, Eurosmart supports the proposal from the Commission to amend article 18.**

# 2. Common specifications

EU Council
*Article 18(3 and 7) - Also refer to recital (41)*

European Parliament
*Article 19 – Also refer to recital (38) (38a) (41)*

Common specifications could be an alternative to harmonised standards to support implementation of this regulation. Common specifications may be very useful to leverage existing industry or sector specific standards for which it has been demonstrated that they meet some or all of the essential requirements of Annex I. As such, common specification could support a quick implementation of the CRA, even if harmonised standards are not available, while limiting the impact on the industry.

The idea whereby harmonised standards should prevail over common specifications and common specifications should be seen as a last-resort option when no harmonised standards are available is too restrictive. **The Common specifications approach should be a complementary option which could address very specific products and use-cases**.

# 3. High-risk AI system

As a general comment enhanced clarity is necessary for the compliance requirements. The interplay between AI act and CRA is not well established.

# 4. Obligations of manufacturer

## 4.1. On components

EU Council
*Article 10(6) First paragraph*

Pursuant to this proposed provision, the manufacturer of the product with digital element shall also ensure that the components vulnerabilities are handled in accordance with Annex I section 2.

Eurosmart would like to highlight that **it may not always be possible**. For instance, in the case where the component is an open-source library, the manufacturer of the product with digital element is not in position to handle vulnerabilities in such components if the provider of the open source library does not (especially security update, but also identification of vulnerability,). In addition, as open-source libraries are likely to be out of the scope of the CRA, their providers will not be required to handle vulnerability in accordance with the CRA. Therefore, this proposed provision is excessive as it puts all

the burden on the manufacturer of the product with digital elements while the component provider may not fall under the CRA. Finally, it shall be noted that vulnerability handling of the product with digital element will indeed consider the components insofar as it is relevant for the product with digital element.

Therefore, Eurosmart recommends removing the following wording:" ~~including its components~~"

## 4.2. Product life-time – Support period

EU Council
*Article 10(6) Second paragraph - Also refer to recital (33-a)*

European Parliament
*Article 10(6) Also refer to recital (32a)*

The expected product lifetime should indeed be determined in accordance with the criteria listed herein. However, other criteria which could also limit the expected product lifetime should also be considered, such as:

(1) the nature of the technology which may limit the possibility to provide security update over time. For instance, hardware-based product may be harder to fix if a vulnerability directly stems from the hardware design of the product; or

(2) the nature of the conformity assessment and reviews of the security of the product with digital elements (Annex I – section 2 – point 3). If In-depth conformity assessment or reviews of the security of product are used (e.g., EU CSA security certification), a higher and deeper knowledge of the product with digital element and its design is provided, combined with a proactive identification of product impacted by vulnerabilities, which in turn is prone to spot any vulnerabilities.

Therefore, Eurosmart recommends adding the above-mentioned criteria for the definition of the expected product lifetime.

## 4.3. Security update

EU Council
*Article 10(6) Fourth paragraph*

It should be clarified from when the security update should be made available for a duration of 10 years. Would either the placing on the market or the release of the security update be considered?

European Parliament
*Article 10(6) Annex I – section 1 – item (3)(a and b)- Also refer to recital (32b)*

Automatic security updates by default are not possible in some cases. Some products with digital elements may not be able to automatically install security update, especially because their connectivity depends on the user which may not always connect them (e.g., payment card).

## 4.4. Access to the source code to other undertakings extending vulnerability handling services

European Parliament
*Article 10(6a)- Also refer to recital (32c)*

Where the support period is shorter than five years and the handling of vulnerabilities has ended, the vulnerability handling service should be managed by a third-party**.** For This provision may violate the IP of manufacturer as well as the freedom to decide on an appropriate vulnerability handling period. This provision may conflict with sectorial certification schemes and with national laws limiting technology transfer.

In addition, the nature of the technology may limit the possibility to provide security update over time. For instance, hardware-based product may be harder to fix on the long term if a vulnerability directly stems from the hardware design of the product.

Therefore, Eurosmart recommends removing this statement.

## 4.5. Subsequent versions of a software product

EU Council
*Article 10(6a)*

Eurosmart very much welcomes this provision. It may be very useful for manufacturers which may have placed on the market several versions of a software and that would like to alleviate the burden of security update preparation **by only issuing security updates for the latest version.**

# 5. List of essential requirements

## 5.1. Distinguish obligations for placing on the market and obligations during the whole product lifetime

EU Council
*Article 10(12)*

European Parliament
*Article 10(12)*

Eurosmart recommends clarifying which of the essential requirements of Annex I – section 1 should be met from the placing on the market over the expected product lifetime (see dedicated comment on that point). Eurosmart recommends bringing clarification on that point.

See also section 6.3 of this document (definition of essential requirement).

## 5.2. SBOM - Information format

Council
*Article 10(15)*

The format of the information and instructions referred to in Annex II should be defined as soon as possible to provide visibility to industry, which will be substantially impacted by the CRA. Therefore, the definition of this format should not be postponed after the adoption of the text but defined in the course of the adoption of the regulation.

Eurosmart recommends defining in the regulation the format of the information and instructions referred to in Annex II, and not postponing it after the adoption of the regulation.

European Parliament
*Article 10(15)*

Format and element of SBOM, format and procedure of notification etc. are technical documents by essence. As they are not providing any additional political aspect to the CRA, Eurosmart recommends relying on **implementing acts** rather than delegated acts.

# 6. Reporting obligations

## 6.1. Limitation in time

EU Council – European Parliament
*Article 11- Also refer to recital (34) and (35)*

The reporting obligations introduced in this article should be limited in time. Under the current version, they are perpetual, which is not acceptable for manufacturers. Manufacturers should not be required to abide by these obligations decades after the products with digital elements are not produced anymore.

Therefore, Eurosmart recommends introducing a limitation in time for the reporting obligations.

## 6.2. No corrective or mitigating measures available

European Parliament
*Article 11(1)- Also refer to recital (34) and (35)*

Eurosmart very much welcomes the addition covering the case of notified vulnerability which does no corrective or mitigating measures available. In such cases, the vulnerability should remain confidential.

## 6.3. Notification procedures – actively exploited vulnerabilities

European Parliament
*Article 11(1a) (1b)*

Eurosmart very much welcomes this new approach for the notification of **actively exploited vulnerability**, which leaves more time to the manufacturer to collect and analyse information.

However, Eurosmart believes, the deadline should be extended.

Moreover Eurosmart supports the provision that acknowledges notified vulnerability should only be made public once corrective or mitigation measures – if possible – have been put in place.

## 6.4. Notification of significant incidents

European Parliament
*Article 11(2) - Also refer to recital (19) and recital (35)*

Eurosmart very much welcomes the proposal to limit the notification to significant incidents. This approach will alleviate the burden for manufacturer while ensuring that only relevant and useful information about incidents is notified. This new approach for the notification of significant incident, which leaves more time to the manufacturer to collect and analyse information.

However, Eurosmart believes, **the deadline should be extended**.

## 6.5. Information to the impacted users

European Parliament
*Article 11(4)*

Eurosmart raises several concerns regarding the provision of this article.

First, it may be difficult for manufacturer to inform users, as he may not know who the users are, especially when the products with digital elements are sold through distributors.

In addition, informing users about a significant incident having an impact on the security of the product with digital elements may raise substantial issues. First it may put at risk industrial and/or trade secrets belonging to the manufacturer. Also, such information may be exploited by malicious entities to carry out cyber-attacks on products with digital elements that have not been fixed, or whose users have not applied mitigation measures. In such situations it is usually better to set up corrective measures without any further information to the users to limit the risks.

Therefore, Eurosmart recommends removing the obligation for manufacturer to inform users about a significant incident having an impact on the security of the product with digital elements, and instead leave it to the CSIRT or the ENISA to decide whether the users should be informed.

# 7. Definitions

## 7.1. Data

EU Council - European Parliament
*Article 3(6) – Also refer to Recital (7)*

Data, when processed by another software or hardware could be understood by national authorities in the light of the definition provided for in article 3(6) as being a "computer code" (For example a word file, or a movie on a DVD, processed by a software to trigger some specific actions).

It seems it is not the intention of the text to also cover data whether formatted in machine-readable format or not. However, this ambiguity could lead to major divergence of implementation of this text within EU.

Therefore, Eurosmart believes a clarification should be brought in that regards to remove any ambiguity and risk of divergence of implementation with EU. Thus Eurosmart recommends adding the following text **within recital (7):**

- "Data (personal or non personal) whether formatted in a machine readable language or not is not a software."

## 7.2. Actively exploited vulnerability

EU Council
*Article 3(39) - Also refer to recital (19a)*

The proposed definition of "actively exploited vulnerability" seems broader than the one initially proposed by the European Commission, as now unsuccessful attempts are also included. This broader definition raises legal concerns.

Only attempts for which the consequences are visible are likely to be noticed, meaning those that are successful. In contrast, unsuccessful attempts, without any consequences are very likely not to be noticed. Therefore, it seems very difficult for the manufacturer from a practical standpoint to establish and identify unsuccessful attempts of exploitation of vulnerabilities.

Therefore, Eurosmart recommends to only include in the definition of **"actively exploited vulnerability successful attempts"**.

## 7.3. Cyber threat

European Parliament
*Article 3(39a)*

Eurosmart very much welcomes this definition which was missing.

## 7.4. Essential requirements

### Council

*Annex I section 1*

The content of Annex I gathers several types of essential requirements which may be classified as follows:

- Essential requirements applicable for the design of the product with digital elements and before its placing on the market : 1; 3(h) and 3(i);
- Essential requirements applicable at the placing on the market of the product with digital elements: 3(a), 3(aa) and 3(aaa);

Regarding the rest of the essential requirements (3(aaa), 3(b), 3(c ), 3(d), 3(e ), 3(f ), 3(g) ), Eurosmart recommends these essential requirements to be met at the placing on the market and not over the expected product lifetime.

According to article 10(12), it seems that these essential requirements should be met from the placing on the market of the product with digital elements over the expected product lifetime. Eurosmart asks for clarifications on this point within Annex I. In addition, for better readability and understanding, Eurosmart suggests reshaping the content of Annex I to clearly distinguish the different types of essential requirements:

- those applicable for the design of the product with digital elements and before its placing on the market;
- those applicable at the placing on the market;
- those applicable from the placing on the market over the expected product lifetime;

### European Parliament – EU Council

*Annex I section 1*

The following essential requirements can't be met by some types of products with digital elements, and rather appears as a feature than an essential requirement:

- "including the possibility to reset the product to its original state" in Council and Parliament 3(a);
- "including a default setting that security updates be installed automatically" in Council 3(a);
- "with a clear and easy- to-use opt-out mechanism." In Council 3(a);
- "set as a default setting – which can be switched off – that security updates are installed automatically on products with digital elements if not installed within a certain timeframe" in Council 3(aaa);
- "through automatic updates by default, but with a clear and easy-to-use opt-out mechanism, and where applicable through the notification of available updates to users, and the option to temporarily postpone them" in Council 3(k);

Therefore, Eurosmart suggests to **either remove them or to keep them and indicate that they are optional features.**

# Annex I

# Comments on the mandate of the European Parliament

| Article/Recital | Eurosmart's feedback | Comments and proposals |
|---|---|---|
| Recital (4) | AGAINST | *"and proportionality for microenterprises and small and medium-sized enterprises"*<br>The addition of this principle is problematic as it implies that the implementation of the provisions of the text would not only depend on the very nature of the product with digital elements, but also on the nature of the manufacturer (microenterprise, SME or not). Yet, the criticality and the need for cybersecurity measures only depends on the products with digital elements, not on the nature of its manufacturer.<br>**Therefore, Eurosmart recommends removing this provision.** |
| Recital (4a) | SUPPORT | Eurosmart very much welcomes this provision |
| Recital (9) | SUPPORT | The examples regarding remote data processing are very useful. Eurosmart very much welcomes this addition. |
| Recital (9) | SUPPORT | The clarification brought regarding difference between the scope of NIS2 and the scope of the CRA regarding remote data processing is very useful. Eurosmart very much welcomes this addition. |
| Recital (9a) | CLARIFICATION NEEDED | The recital talks of "data" alongside "software". Yet, "data" are not covered by the CRA.<br>**Eurosmart would like clarification regarding the reasoning for considering "data" here.** |
| Recital (9a) | SUPPORT | Eurosmart very much welcomes the definition of free and open-source software which is provided herein. |
| Recital (10)<br>Recital (10a) | AGAINST | Eurosmart strongly disagrees with the approach whereby the development model should be considered to assess whether or not a commercial activity is at stake.<br>Eurosmart strongly believes that only the nature of the transaction giving rise to the transfer of ownership of the product with digital elements should be considered, and whether this transaction leads to profit or not. Any other aspect is irrelevant and should not be considered.<br>**Therefore, Eurosmart recommends modifying recital (10) accordingly and removing recital (10a)** |
| Recital (10b) | AGAINST | *"Accepting donations without the intention of making a profit should not be considered to be a commercial activity, unless such donations are made by commercial entities and are recurring in nature."*<br>Eurosmart believes that the sole criteria for determination of commercial transactions should be whether the transaction gives rise to a profit or not. The development model is irrelevant and should not be considered, including the nature of who made the donation.<br>**Therefore, Eurosmart recommends removing this statement.** |
| Recital (10c) | AGAINST | As for Recital (10b) Eurosmart believes that the sole criteria for determination of commercial transactions should be whether the transaction gives rise to a profit or not. The development model is irrelevant and should not be considered, including the nature of who contributes.<br>**Therefore, Eurosmart recommends removing this recital.** |
| Recital (10d) | SUPPORT WITH ADDITION | Eurosmart supports this recital. However, it should be clarified that it is true insofar there are no commercial transactions (i.e. no profit). If there is a commercial transaction, package managers, code hosting and collaboration platforms would fall under this regulation.<br>**Eurosmart recommends adding the clarification** |

| Article/Recital | Eurosmart's feedback | Comments and proposals |
|---|---|---|
| Recital (14b) | SUPPORT | Eurosmart very much welcomes this provision, which will avoid overlap and redundancy for manufacturers. |
| Recital (18) | SUPPORT | Eurosmart believes that it is key to alleviate the conformity tasks by mutualizing as much as possible conformity tasks required by eIDAS and this proposal. Doing so would alleviate the burden for industry and stakeholders thus decrease costs, which would foster the uptake of eIDAS and the wallet.<br><br>**Therefore, Eurosmart supports the presence of this recital, and in particular the second half describing how to mutualize conformity tasks between eIDAS and this proposal.** |
| Recital (19) | SUPPORT | Eurosmart very much welcomes the other clarifications brought in this recital. |
| Recital (19a) | SUPPORT | Eurosmart very much welcomes these clarifications regarding the needed security measures for notifications. |
| Recital (21) | AGAINST | *"in a non-production version"*<br><br>This wording seems misleading, as even for such purposes, a product with digital elements may be produced using the same processes and machines as the ones that will be used for mass production or placing on the market. In addition, the exact meaning of this term is unclear.<br><br>**Therefore, Eurosmart recommends removing this term.** |
| Recital (22) | SUPPORT | Eurosmart very much welcomes these additions which clarify that security updates, minor adjustment of the source code or minor functionality updates should not be considered as substantial changes. This brings clarity to manufacturers while alleviating their burden.<br><br>In addition, Eurosmart supports the proposal to have a guideline on how to determine what constitutes a substantial modification. |
| Recital (22) | CLARIFICATION NEEDED | Eurosmart would like to highlight that software update, security update or patch will most likely take the shape of a software which will be executed by the product with digital element. However, those should not be considered as a product with digital elements themselves.<br><br>**Therefore, Eurosmart recommends clarifying this aspect by a dedicated recital:**<br><br>**"software updates, security updates or patches alone which are intended for products with digital elements are not product with digital elements."** |
| Recital (26) | CLARIFICATION NEEDED | What is the exact meaning of "high-risk" environment?<br><br>Clarification is needed. |
| Recital (27) | CLARIFICATION NEEDED | "For example, Annex III to this Regulation lists products which are defined by their core functionality as general-purpose microprocessors in class I. As a result, general purpose microprocessors are subject to mandatory third-party conformity assessment. This is not the case for other products not explicitly referred to in Annex III to this Regulation which may integrate a general purpose microprocessor."<br><br>**Eurosmart believes some clarifications should be brought to the composition rules.**<br><br>**A product with digital elements may integrate either (1) a product with digital elements (thus placed on the market), or (2) a component – not necessarily placed on the market as supplied internally. In both cases, if the core functionality of such product** |

| Article/Recital | Eurosmart's feedback | Comments and proposals |
|---|---|---|
| | | **with digital elements or component falls into the list defined in Annex III, it should be subject to mandatory conformity assessment as described in Article 24.**<br><br>**In addition, the concept of core functionality should also be further clarified.** |
| Recital (32) | SUPPORT | Eurosmart very much welcomes the clarification made that compliance with all essential requirements related to vulnerability handling applies throughout the support period. |
| Recital (32) | CLARIFICATION NEEDED | In many cases, compliancy with standards required by the markets, procuring authorities or legislation may entail that the product with digital element does not to abide by some essential requirements. This situation should be clearly considered in a dedicated recital.<br><br>**Therefore Euromart recommends to add a recital which clarifies that compliancy to standards may prevail in some cases even if it implies not to abide by all essential requirements.** |
| Recital (32) | AGAINST | International standards cannot be registered as such, Vienna and Frankfort agreements provides that these standards should be "translated" into a European format.<br><br>Moreover, the very nature of international standards is different from the one of harmonised standards and common specifications.<br><br>Harmonised standards and common specifications are technical documents which:<br>- have been approved by the European Commission (through publication in the OJUE for harmonised standards or publication of implementing act for common specifications);<br>- bring presumption of conformity with the essential requirements listed in Annex I, which is confirmed by the approval of the European commission.<br><br>International standards do not meet any of these criteria. These are only technical documents which:<br>- are neither controlled nor approved in any manner by the European Commission;<br>- Are not assessed by European Standardisation Organisation in the course of a standardisation request<br>- do not ensure fulfilment of the essential requirement listed in annex I;<br>- are also substantially prepared by non EU entities, which may take advantage of it to water down or influence cybersecurity requirements made mandatory through this regulation. This approach may be used as a Trojan horse to jeopardize the resilience of the single market.<br><br>**Eurosmart believes, that putting international standards on an equal footing with harmonised standards or common specification is fallacious. However, it is crucial for the swift implementation of the regulation, that both Common specifications and harmonised standards relies on existing international standards.**<br><br>**Therefore, Eurosmart recommends to remove reference to "international standards".** |
| Recital (34) | AGAINST | Eurosmart believes that notified vulnerabilities should not be published by ENISA in the European vulnerability database in order to limit any risk of exploitation by malicious actors.<br><br>**Eurosmart recommends removing this provision** |

| Article/Recital | Eurosmart's feedback | Comments and proposals |
|---|---|---|
| Recital (35c) | SUPPORT | Eurosmart very much welcomes this proposal. Entities and natural persons researching vulnerabilities should not be prosecuted, as they are instrumental to enhance the level of cybersecurity of products with digital elements. |
| Recital (37) | SUPPORT | Eurosmart very much welcomes this proposal. SBOM may be a sensitive information and should not be made public. |
| Recital (38) | AGAINST | *"The standardisation process should ensure a balanced representation of interests and effective participation of civil society stakeholders, including consumer organisations."*<br><br>This is the very nature of standardisation process; therefore this addition is useless and irrelevant. Eurosmart recommends to remove it.<br><br>*"International standards should also be taken into account, in order to simplify the development of harmonised standards and the implementation of this Regulation, as well as to reduce non-tariff technical barriers to trade."*<br><br>This statement seems useless, as international standards will always be considered by an ESO which has been tasked with a standardisation request. This is achieved naturally thanks to existing agreements (e.g. Vienna's agreement, Frankfurt agreement) between ESOs (which can receive standardisation request for harmonised standards) and bodies preparing international standards (ISO, ITU, IEC), which avoids duplication of work and competition in standards and supports rationalisation of standards.<br><br>**Eurosmart recommends to remove it.** |
| Recital (38a) | AGAINST | Common specifications could be an alternative to harmonised standards to support implementation of this regulation. Common specifications may be very useful to leverage existing industry or sector specific standards for which it has been demonstrated that they meet some or all of the essential requirements of Annex I. As such, common specification could support a quick implementation of the CRA, even if harmonised standards are not available, while limiting the impact on the industry. |
| Recital (41) | AGAINST | This provision is underpinned by the idea whereby (1) harmonised standards should prevail over common specifications and (2) common specifications should be seen as a last-resort option, when no harmonised standards are available.<br><br>Eurosmart believes this approach of common specification is far too limitative. Common specifications may also be very useful to leverage existing industry or sector specific standards for which it has been demonstrated that they meet some or all of the essential requirements of Annex I. As such, common specification could support a quick implementation of the CRA, while limiting the impact on the industry.<br><br>**Therefore Eurosmart recommends reviewing the whole recital accordingly.**<br><br>In addition, for the reasons described above, not only international standards should be taken into account, but also all existing or legacy industrial specification. |
| Article 2(3a) | AGAINST | This provision is useless as it is already contained in point 1 of the same article. It is irrelevant to create a specific provision for a particular case.<br><br>Eurosmart recommends to delete this statement. |
| Article 2(4a) | SUPPORT | Eurosmart very much welcomes exemptions for spare parts. This will ensure durability of product with digital elements. |

| Article/Recital | Eurosmart's feedback | Comments and proposals |
|---|---|---|
| Also refer to recital (14a) | | |
| Article 3(6) | CLARIFICATION NEEDED | The meaning of computer code is unclear and should be further defined. |
| Article 3(6)<br><br>Recital (7) | CLARIFICATION IS NEEDED | Data, when processed by another software or hardware could be understood by national authorities in the light of the definition provided for in article 3(6) as being a *"computer code"* (For example a word file, or a movie on a DVD, processed by a software to trigger some specific actions).<br>It seems it is not the intention of the text to also cover data whether formatted in machine-readable format or not. However, this ambiguity could lead to major divergence of implementation of this text within EU.<br>Therefore, Eurosmart believes a clarification should be brought in that regards to remove any ambiguity and risk of divergence of implementation with EU.<br>**Thus Eurosmart recommends adding the following text within recital (7):**<br>***"Data (personal or non personal) whether formatted in a machine readable language or not is not a software."*** |
| Article 3(31)<br><br>Also refer to recital (22) | SUPPORT | Eurosmart very much welcomes these additions which clarify that security updates should not be considered as substantial changes. This brings clarity to manufacturers while alleviating their burden. |
| Article 3(39a) | SUPPORT | Eurosmart very much welcomes the addition of this definition which was missing. |
| Article 4(2)<br><br>Also refer to recital (20) | SUPPORT | Eurosmart very much welcomes this clarification |
| Article 4(3) | AGAINST | Even in such cases, unfinished software may be made available against payment as some costs may have to be incurred by the manufacturer which could be charges to the customer (e.g. translation, specific adaptation to fit the customer IT systems…).<br>**Therefore Eurosmart recommends removing the obligation of "free of charge".** |
| Article 4(3a) | SUPPORT | Eurosmart very much welcomes this clarification |
| Article 6(1) | SUPPORT | Eurosmart very much welcomes this addition which provides clarification regarding composition rules. |
| Article 6(2) | AGAINST | Eurosmart believes this process for amending Annex III is too rigid and is not flexible enough to allow swift and quick actions in case of emergency. |

| Article/Recital | Eurosmart's feedback | Comments and proposals |
|---|---|---|
| Also refer to recital (27) | | **Therefore, Eurosmart recommends removing this planning and revert to initial text.** |
| Article 6(2) | AGAINST | Clear criteria for the classification of a product as critical product of class I or class II are missing. In order to bring visibility to the industry, such criteria should be well defined in the regulation, as they will guide any further modifications of III. |
| Article 6(3)<br><br>Also refer to recital (27) | AGAINST | For the smooth implementation of the CRA and to ensure legal certainty the definitions of product categories connot be provided 6 months after the date of entry into force of this regulation. The definitions, together with product categories are absolutely needed by the industry so that it could adapt as soon as possible to the CRA, whose impacts will be substantial.<br><br>**Eurosmart recommends providing the definitions at the same time as the regulation, and also have them subject to the same scrutiny process as the regulation itself.** |
| Article 6(5) | AGAINST | Eurosmart recommends prioritizing the implementation of the CRA principles like implementation of Essential Cybersecurity Requirements on those product categories where the conformance mechanisms are not yet regular practice. Certification obligation in the CRA context for all high-end security products will complexify existing high-level evaluation processes. Several types of evaluations are already required for various sectors and have maintained products at the State-of-the-Art for years through the assessment of advanced and sector-specific security requirements.<br><br>Eurosmart invites the co-legislators to reconsider the European Council proposal focusing on certification obligation for all high-end security products as laid down in Annex IIIa of the proposal.<br>In the meantime, effort should be made to recognised EU cybersecurity certification schemes as a possibility to demonstrate conformity with the CRA essential requirements. |
| Article 6a<br><br>Article 10(15)<br><br>Article 17a(3)<br><br>Article 19(2)<br><br>Article 22(6)<br><br>Article 41(9a)<br><br>Article 41(11) | SUPPORT | Eurosmart very much welcomes the proposal to set up such an expert group to assist the European Commission.<br><br>In addition, Eurosmart, which represents the European digital security industry, would be delighted to join this expert group as part of representants of relevant economic operators to bring its expertise. |

| Article/Recital | Eurosmart's feedback | Comments and proposals |
|---|---|---|
| Also refer to recital (27a), recital (62) and recital (68) | | |
| Article 6a(1)(c ) | AGAINST | This provision seems to give over representation and privileges to free and open-source community, while (1) free and open source is only a type of product with digital elements among many others, and (2) in most cases free and open source is likely not to fall within the scope of the CRA as it will not be the subject of commercial activities.<br>Instead the free and open source community should be represented as part of the relevant economic operators under b).<br>**Therefore Eurosmart recommends removing the explicit mention to free and open source community** |
| Article 6a | SUPPORT WITH ADDITION | Eurosmart believes common specification may also be very useful to leverage existing industry or sector specific standards for which it has been demonstrated that they meet some or all of the essential requirements of Annex I. As such, common specification could support a quick implementation of the CRA, while limiting the impact on the industry. This aspect should also be discussed within the expert group.<br>**Therefore, Eurosmart recommends adding the following item to the list:**<br>**"(i) the opportunity to convert existing industry or sector specific standards into common technical specifications".** |
| Article 9a(1)<br><br>Also refer to recital (18a) | AGAINST | *"and an appropriate support period"*<br><br>Eurosmart would like to highlight that the support period may be limited by some factors such as:<br>1) the nature of the technology which may limit the possibility to provide security update over time. For instance, hardware based product may be harder to fix if a vulnerability directly stems from the hardware design of the product; or<br>2) the nature of the conformity assessment and reviews of the security of the product with digital elements (Annex I – section 2 – point 3). If In-depth conformity assessment or reviews of the security of product are used (e.g. EU CSA security certification), a higher and deeper knowledge of the product with digital element and its design is provided, combined with a proactive identification of product impacted by vulnerabilities, which in turn is prone to spot any vulnerabilities.<br>**Therefore Eurosmart recommends removing the following statement "and an appropriate support period"** |
| Article 9a(2)<br><br>Also refer to recital (18a) | AGAINST | This specific provision seems absolutely useless, as it is the very purpose of the whole regulation to ensure these objectives are met, regardless who procured the product with digital elements. There is no point in requiring a particular treatment for Member States.<br><br>Therefore Eurosmart recommends removing this provision. |
| Article 10(2) | CLARIFICATION NEEDED | The content and shape of the cybersecurity risk assessment still remain unknown, despite it is crucial to conduct the conformity assessment tasks. |

| Article/Recital | Eurosmart's feedback | Comments and proposals |
|---|---|---|
| | | Eurosmart recommends to provide clear details about the content and shape of the cybersecurity risks assessment in this article. |
| Article 10(4)<br><br>Also refer to recital (10e) | SUPPORT | Eurosmart believes that the addition regarding obligation of due diligence even in the case of free and open source software which has not be supplied in the course of a commercial transaction is positive. |
| Article 10(4) | SUPPORT | Eurosmart also very much welcomes the obligation regarding the handling of vulnerabilities in a component of the product with digital elements. |
| Article 10(4a) | SUPPORT | Eurosmart very much welcomes this proposal which makes sure that the manufacturer of the product with digital elements gets all necessary information relating to the components used. |
| Article 10(6)<br><br>Also refer to recital (32a) | SUPPORT | The support period should indeed be determined in accordance with the criteria listed herein. However, other criteria which could also limit the support period should also be considered, such as:<br>(1) the nature of the technology which may limit the possibility to provide security update over time. For instance hardware based product may be harder to fix if a vulnerability directly stems from the hardware design of the product; or<br>(2) the nature of the conformity assessment and reviews of the security of the product with digital elements (Annex I – section 2 – point 3). If In-depth conformity assessment or reviews of the security of product are used (e.g. EU CSA security certification), a higher and deeper knowledge of the product with digital element and its design is provided, combined with a proactive identification of product impacted by vulnerabilities, which in turn is prone to spot any vulnerabilities.<br>Therefore Eurosmart recommends adding the following criteria for the definition of the support period:<br>(1) the nature of the technology which may limit the possibility to provide security update over time. For instance hardware based product may be harder to fix if a vulnerability directly stems from the hardware design of the product; or<br>(2) (2) the nature of the conformity assessment and reviews of the security of the product with digital elements (Annex I – section 2 – point 3). If In-depth conformity assessment or reviews of the security of product are used (e.g. EU CSA security certification), a higher and deeper knowledge of the product with digital element and its design is provided, combined with a proactive identification of product impacted by vulnerabilities, which in turn is prone to spot any vulnerabilities. |
| Article 10(6)<br><br>Annex I – section 1 – item (3)(ab)<br>Also refer to recital (32b) | AGAINST | Eurosmart disagrees with the requirement to have automatic security updates by default.<br>**Some products with digital elements may not be able to automatically install security update, especially because their connectivity depends on the user which may not always connect them (e.g. payment card).** |
| Article 10(6a) | AGAINST | This provision may violate the IP of manufacturer as well as its freedom, and may conflict with national laws limiting technology transfer. |

| Article/Recital | Eurosmart's feedback | Comments and proposals |
|---|---|---|
| Also refer to recital (32c) | | In addition, the nature of the technology may limit the possibility to provide security update over time. For instance hardware based product may be harder to fix on the long term if a vulnerability directly stems from the hardware design of the product.<br>**Therefore, Eurosmart recommends to remove this statement.** |
| Article 10(8) | SUPPORT | Eurosmart welcomes this proposal. |
| Article 10(12) | SUPPORT | Eurosmart very much welcomes this proposal |
| Article 10(12) | CLARIFICATION NEEDED | It should be clarified which of the essential requirements of Annex I – section 1 should be met from the placing on the market over the support period (see dedicated comment on that point). **Eurosmart recommends bringing clarification on that point.** |
| Article 10(15)<br><br>Article 11(5)<br><br>Article 50<br><br>Also refer to recital (62) | AGAINST | All of these acts are technical in nature, and not legal (format and element of SBOM, format and procedure of notification…). Therefore, Eurosmart recommends to rely on implementing acts and not delegated acts. |
| Article 10(15) | AGAINST | The format of the information and instructions referred to in Annex II should be defined as soon as possible to provide visibility to industry, which will be substantially impacted by the CRA. Therefore, the definition of this format should not be postponed after the adoption of the text, but defined in the course of the adoption of the regulation.<br>**Eurosmart recommends defining in the regulation the format of the information and instructions referred to in Annex II, and not postponing it after the adoption of the regulation.** |
| Article 11<br><br>Also refer to recital (34) and (35) | AGAINST | The reporting obligations introduced in this article should be limited in time. Under the current version, they are perpetual, which is not acceptable for manufacturers. Manufacturers should not be required to abide by these obligations decades after the products with digital elements are not produced anymore.<br>**Therefore, Eurosmart recommends introducing a limitation in time for the reporting obligations.** |
| Article 11(1) | SUPPORT | Eurosmart very much welcomes the addition covering the case of notified vulnerability which does no corrective or mitigating measures available. In such cases, the vulnerability should remain confidential. |
| Article 11(1a) | SUPPORT | Eurosmart very much welcomes this new approach for the notification of actively exploited vulnerability, which leaves more time to the manufacturer to collect and analyse information.<br>However, Eurosmart believes, the deadline should be extended. |

| Article/Recital | Eurosmart's feedback | Comments and proposals |
|---|---|---|
| Article 11(1b) | SUPPORT | Eurosmart very much welcomes this addition which acknowledges that notified vulnerability should only be made public once corrective or mitigation measures – if possible – have been put in place. |
| Article 11(2)<br><br>Also refer to recital (19) and recital (35) | SUPPORT | Eurosmart very much welcomes the proposal to limit the notification to significant incidents. This approach will alleviate the burden for manufacturer while ensuring that only relevant and useful information about incidents is notified. |
| Article 11(2) | SUPPORT | Eurosmart very much welcomes the clarification whereby the mere act of notification shall not subject the notifying entity to increased liability. |
| Article 11(2a) | SUPPORT | Eurosmart very much welcomes the proposed definition of significant incident. |
| Article 11(2b) | SUPPORT | Eurosmart very much welcomes this new approach for the notification of significant incident, which leaves more time to the manufacturer to collect and analyse information.<br><br>However, Eurosmart believes, the deadline should be extended. |
| Article 11(2c) | SUPPORT | Eurosmart very much welcomes this proposal which alleviate the burden of operators also falling under NIS2. |
| Article 11(2e)<br><br>Also refer to recital (4) | AGAINST | Eurosmart strongly disagrees with this proposal. The cybersecurity requirements shall be the same regardless whether the manufacturer is a microenterprise or a SME or not. Doing so could create substantial security breaches and impair the global objective of the text. |
| Article 11(4) | AGAINST | Eurosmart has several concerns regarding the provision of this article.<br><br>First, it may be difficult for manufacturer to inform users, as he may not know who the users are, especially when the products with digital elements are sold through distributors.<br><br>In addition, informing users about a significant incident having an impact on the security of the product with digital elements may raise substantial issues. **First it may put at risk industrial and/or trade secrets belonging to the manufacturer**. **Also such information may be exploited by malicious entities to carry out cyber-attacks on products with digital elements that have not been fixed, or whose users have not applied mitigation measures. In such situations it is usually better to set up corrective measures without any further information to the users in order to limit the risks.**<br><br>**Therefore, Eurosmart recommends to remove the obligation for manufacturer to inform users about a significant incident having an impact on the security of the product with digital elements, and instead leave it to the CSIRT or the ENISA to decide whether or not user should be informed.** |
| Article 11(4a) | SUPPORT | Eurosmart very much welcomes this proposal |
| Article 11(6a) | SUPPORT | Eurosmart very much welcomes this proposal which will alleviate the burden for manufacturers. |

| Article/Recital | Eurosmart's feedback | Comments and proposals |
|---|---|---|
| Also refer to recital (35b) | | |
| Article 11a | SUPPORT | Eurosmart very much welcomes this new article which provide a legal framework for voluntary notification |
| Article 11b | SUPPORT | Eurosmart very much welcomes this proposal, however such provisions seems already included in the essential requirement defined in Annex I – section 2 item 5 which mandates a coordinated vulnerability disclosure policy. |
| Article 13(3) | CLARIFICATION NEEDED | This provision should be aligned with the one in article 14(3) |
| Article 13(6) | CLARIFICATION NEEDED | This provision should be aligned with the one in article 14(4) |
| Article 13(7) | CLARIFICATION NEEDED | This provision should be aligned with the one in article 10(8) |
| Article 13(9) | CLARIFICATION NEEDED | This provision should be aligned with the one in article 14(6) |
| Article 16<br>First paragraph | CLARIFICATION NEEDED | In accordance with the definition of manufacturer (article 3(18) ), a natural or legal persons placing a product with digital elements on the market under his or her name or trademark shall be considered a manufacturer for the purposes of this Regulation.<br>**The content of the first paragraph shall be amended accordingly as follows:**<br>**"A natural or legal person, other than the manufacturer, the importer or the distributor, which places a product with digital elements on the market under his or her name or trademark or carries out a substantial modification of the product with digital elements and makes it available on the market, shall be considered a manufacturer for the purposes of this Regulation."** |
| Article 17a(2) | SUPPORT WITH ADDITION | Eurosmart very much welcomes the introduction of such article which provides for guidelines in order to support economic operators in the implementation of this regulation. However, the timeframe for the publication of such guidelines (12 months) is too long. Such guidelines should be made available as soon as possible, as the effort required to comply with this regulation will be very substantial for economic operators.<br>**Therefore Eurosmart recommends to set the deadline to 2 months.** |
| Article 17a(2)(b) | AGAINST | Eurosmart disagrees with this proposal. The criteria used to determine how critical products with digital elements are placed in classes I or II shall be part of the legal text and shall be defined in article 6. They shall not be deferred to guidelines. |
| Article 17a(2)(d) | AGAINST | The content and shape of the cybersecurity risk assessment is crucial to conduct the conformity assessment tasks and shall be defined in article 10(2). It shall not be deferred to guidelines.<br>**Eurosmart recommends providing clear details about the content and shape of the cybersecurity risks assessment in article 10(2).** |
| Article 18(1) | AGAINST | This addition is not in line with the way harmonised standards are managed. |

| Article/Recital | Eurosmart's feedback | Comments and proposals |
|---|---|---|
| | | 1/It is up to the ESO(s) which is tasked to execute the standardisation request to take into account existing or upcoming international standards. This is achieved naturally thanks to existing agreements (e.g. Vienna's agreement, Frankfurt agreement...) between ESOs (which can receive standardisation request for harmonised standards) and bodies preparing international standards (ISO, ITU, IEC), which avoids duplication of work and competition in standards and supports rationalisation of standards.<br>2/ harmonised standards prepared following a standardisation request shall also meet some formal and precise criteria (https://boss.cen.eu/developingdeliverables/pages/en/pages/enforojeu/ & HAS assessment process (cen.eu)). Yet, international standards may not meet them, implying to draft an ad hoc harmonised standard.<br>Therefore Eurosmart suggests removing this statement. |
| Article 18(4)<br><br>Article 50<br><br>Also refer to recital (39) and recital (62) | AGAINST | Eurosmart believes that implementing act and not delegated act should be used as the very nature of this act is technical and not legal.<br>The nature is similar to the publication of a harmonised standard in the OJUE.<br>**Therefore Eurosmart suggests reverting to an implementing act.** |
| Article 18(4)<br><br>Article 24(2)<br><br>Also refer to recital (39) | SUPPORT | Eurosmart very much welcomes this provision recognizing that there should not be any obligation to carry out a third-party conformity assessment where a cybersecurity certificate pursuant to regulation 2019/881 at level "substantial" or "high" is obtained. |
| Article 19<br><br>Also refer to recital (41) | AGAINST | This proposal is underpinned by the idea whereby (1) harmonised standards should prevail over common specifications and (2) common specifications should be seen as a last-resort option, when no harmonised standards are available.<br>Eurosmart believes this approach of common specification is far too limitative. Common specifications may also be very useful to leverage existing industry or sector specific standards for which it has been demonstrated that they meet some or all of the essential requirements of Annex I. As such, common specification could support a quick implementation of the CRA, while limiting the impact on the industry.<br>**Therefore Eurosmart recommends reviewing the whole recital and article accordingly.** |
| Article 19<br><br>Article 50 | AGAINST | Eurosmart believes that implementing act and not delegated act should be used for common specification, as the very content is technical and not legal.<br>The nature is similar to the publication of a harmonised standard in the OJUE.<br>**Therefore Eurosmart suggests reverting to an implementing act.** |

| Article/Recital | Eurosmart's feedback | Comments and proposals |
|---|---|---|
| Also refer to recital (41) and recital (62) | | |
| Article 22(6)<br><br>Also refer to recital (63) | SUPPORT | Eurosmart supports the possibility to also include harmonised labels and labelling scheme on product with digital elements. It would be very useful to affix label denoting a European security certification pursuant to the regulation 2019/881, or the label defined by ENISA. |
| Article 23(2) | SUPPORT | Eurosmart very much welcomes this proposal which limits in time the obligation to continuously update the technical documentation. |
| Article 23(5) | AGAINST | Eurosmart strongly disagrees with this proposal. The requirements regarding the technical documentation should be the same regardless whether the manufacturer is a microentreprise or a SME or not.<br><br>If simplification in technical documentation is possible it should be available to all. |
| Article 24(1)<br><br>Also refer to recital (62) | SUPPORT | Eurosmart very much welcomes the addition of bullet (ca), which makes clear that a security certification scheme pursuant to regulation 2019/881 can be used to demonstrate conformity. |
| Article 24(2a) – first sentence<br><br>Also refer to recital (45) | AGAINST | The proposal requires that harmonised standards, common specifications or cybersecurity certification schemes be in place for a minimum period of time (here 6 months) before they could be used for a conformity assessment.<br><br>Eurosmart does not agree with this approach and believes it will impair the use of harmonised standards, common specifications or cybersecurity certification schemes. As harmonised standards, common specifications or cybersecurity certification schemes will bring a **presumption of conformity** with the essential requirements listed in Annex I, it is very likely that they will be preferred by manufacturer in order to reduce the burden of conformity assessment. Therefore, they should be usable as soon as possible.<br><br>**Eurosmart believes this proposal will be detrimental to the smooth implementation of this regulation, and recommends to remove it.** |
| Article 24(2) – second sentence | AGAINST | This proposal creates a major loophole in the cybersecurity assessment of class I product. It means that as long as harmonised standards, common specifications or cybersecurity certification schemes are not in place for a minimum period of time (here 6 months), these products will be assessed as if they were non critical products with digital elements. It means that they could be assessed using a self assessment (module A or EU declaration of conformity pursuant to regulation 2019/881) using any technical documents. This creates substantial cybersecurity risks on class I products, while the purpose of the text is to circumvent them.<br><br>Therefore Eurosmart recommends removing this proposal. |
| Article 24(3)<br><br>Also refer to recital (39a) | SUPPORT | Eurosmart very much welcomes this proposal. Any missing cybersecurity certification scheme pursuant to regulation 2019/881 which is identified should be prepared, and the ENISA should be tasked to so so |

| Article/Recital | Eurosmart's feedback | Comments and proposals |
|---|---|---|
| Article 24a | SUPPORT WITH ADDITION | Such MRA should only be concluded provided all the requirements enacted in this text are met by the other party. Eurosmart recommends clarifying this aspect in this article. |
| Article 27(6a) | AGAINST | Such provision creates distortion between microentreprise, SME and the others. If minimisation of administrative burden and fees is possible it should be available to all.<br>**Therefore Eurosmart recommends applying this article not only to microenterprise and SME but to any manufacturer.** |
| Article 28(1a)<br>Article 29(7a)<br>Also refer to recital (53) and recital (53a) | SUPPORT | Eurosmart very much supports this provision emphasing the importance of taking measures to avoid bottlenecks. |
| Article 29(5)<br>Article 29(10) | SUPPORT WITH ADDITION | Eurosmart would like to highlight that these provisions regarding personnel (professional secrecy, professional integrity, free from pressures and inducements) as well as regarding confidentiality (article 52) can only be enforced and guaranteed provided each member of the personnel can be held liable if he doesn't abide by these rules. Therefore, it implies that this regulation shall also apply in the country where the personnel at stake is located. If not, members of the personnel may not abide by these rules as they would not perceive any legal risks.<br>Yet, article 29 allows the personnel to be located outside the EU.<br>Therefore Eurosmart recommends adding the following requirement in article 29:<br>"All personnel shall be located within EU." |
| Article 35 | CLARIFICATION NEEDED | The consequences of the restriction, suspension or withdrawal of the notification of the notified body on the conformity assessment of a product with digital element should be further clarified:<br>• What happens to ongoing conformity assessments? Is it the responsibility of the notifying authority to assign them to another notified body?<br>• What happens to product with digital elements, which are monitored after initial conformity assessment by that notified body? Is it the responsibility of the notifying authority to assign them to another notified body?<br>Eurosmart would like clarification on that point |
| Article 37(4) | CLARIFICATION NEEDED | "conformity certificate" is not defined anywhere in the text, and it is unclear what it designates. As per our understanding, certificate of conformity designates any of the followings:<br>• EU type examination certificate (where module B is used);<br>• Approval decision (where module H is used) |

| Article/Recital | Eurosmart's feedback | Comments and proposals |
|---|---|---|
| | | Eurosmart suggests adding a definition of "conformity certificate" in article 3 |
| Article 37(5)<br>Article 37(6) | CLARIFICATION NEEDED | Eurosmart would like clarifications regarding the consequences of the suspension or restriction of a conformity certificate. What are the consequences for the product with digital elements? |
| Article 38(1)<br>Bullet (a ) | SUPPORT WITH ADDITION | Eurosmart suggests using the wording "conformity certificate" |
| Article 42 | AGAINST | Eurosmart recommends that this provision should be exercised within the limits of article 52 about confidentiality. |
| Article 49(3)<br><br>Also refer to recital (61) | SUPPORT WITH ADDITION | Eurosmart also recommends considering a second criteria for the sweeps, which is the type of conformity assessment procedure mostly used for a category of products with digital elements. As security certification pursuant to EU CSA brings a higher level of confidence - in particular because it is a **white box approach**, unlike conformity modules, categories of products with digital elements where module A, module B+C or module H are mostly used should also be given the priority by sweeps. |
| Article 53(1) | AGAINST | Such provision creates distortion between micro-entreprise, SME and the others. Financial capabilities of any enterprises, whether it is a microenterprise or a SME or not should be considered.<br>**Therefore Eurosmart recommends only referring to the financial capabilities of enterprises, without any particular mention to microenterprise or SME.** |
| Article 53(3) | AGAINST | Pursuant to article 10(6), compliancy with Annex I – section 2 is only required for the support period, while article 10(1) indicates that compliancy with Annex I – Section 1 is only required at the placing on the market. Therefore, the requirement to comply with Annex I is limited in time.<br>Therefore, this provision seems excessive and useless: "The non-compliance with the essential cybersecurity requirements laid down in Annex I should lead to an administrative fine […]". It is excessive as this wording ignores the limitation in time as enacted in article 10(6), and thus would mean that the essential requirements of Annex I would be mandated forever, even well after the expected product lifetime. It would create a major legal and financial risks for manufacturers which could even deter some of them to pursue their activities. In addition, it is also useless as compliancy with Annex I is included in the provisions of article 10 which is explicitly quoted.<br>**Therefore Eurosmart recommends amending this provision as follows:**<br>**"The non-compliance with ~~the essential cybersecurity requirements laid down in Annex I and~~ the obligations set out in Articles 10 and 11 shall be subject to administrative fines of up to 15 000 000 EUR or, if the offender is an undertaking, up to 2.5 % of the its total worldwide annual turnover for the preceding financial year, whichever is higher."** |
| Article 53(6)(aa) | SUPPORT | Eurosmart very much welcomes this addition. |
| Article 53a | SUPPORT | Eurosmart very much welcomes this addition. |

| Article/Recital | Eurosmart's feedback | Comments and proposals |
|---|---|---|
| Article 55(3) | CLARIFICATION NEEDED | **This provision is unclear and seems in contradiction with article 57.** It contravenes with the general principle of *non-retroactivity of law.*<br><br>Article 55(3) reads the following:<br><br>*"By way of derogation from paragraph 2, the obligations laid down in Article 11 shall apply to all products with digital elements that fall within the scope of this Regulation that have been placed on the market **before** [XXX]"*<br><br>While article 57 reads the following:<br><br>*"However Article 11 shall apply **from** [18 months after the date of entry into force of this Regulation]."*<br><br>**Clarifications are needed.** |
| Article 55(3a)<br><br>Also refer to recital (15) | SUPPORT | Eurosmart very much welcomes this provision, which will ensure a smooth migration for manufacturer from the RED legal framework to the CRA. |
| Article 56(2) | SUPPORT | Eurosmart very much welcomes this addition. |
| Article 57<br><br>Also refer to recital (69) | SUPPORT WITH ADDITION | Eurosmart very much welcomes this new timeframe for the application of this regulation. It leaves more time for stakeholders to be ready for the implementation of the CRA.<br><br>Nevertheless, Eurosmart rather suggests setting the date for application of article 11 to 24 months after entry into force of this regulation. |
| Article 57 | CLARIFICATION NEEDED | The implementation of the text should be carefully analysed.<br><br>Many companies, qualifying as "manufacturers", are suppliers of customers which also qualify as "manufacturers". This is the case where the customer (1) applies its own brand on the products with digital elements, (2) subcontracted the development, or (3) carried out substantial modification to the products with digital elements.<br><br>This element should be borne in mind when defining the timeline for the implementation of the text.<br><br>In that case, both the supplier and the customer should abide by the deadlines set forth in article 57, as both will place products with digital elements on the market (as they are both manufacturers). It entails that the supplier should be ready well ahead of time so that its customer could be ready on time.<br><br>This means that time enough should be left once all the supporting documentation has been published (Implementing acts, delegated acts,…) and processes are in place (conformity assessment,…) so that:<br><br>(1) the supplier could be ready and have compliant products with digital elements;<br><br>(2) the customer could sell all its stocks which does not comply; |

| Article/Recital | Eurosmart's feedback | Comments and proposals |
|---|---|---|
| | | (3) the customer could procure the new products with digital elements - which are compliant - to the supplier<br>If the time left to manage this transition is not enough, it may result in substantial disruption in supply chain, as well as financial loss.<br>**Therefore Eurosmart recommends to let at least 3 years once all the supporting documentation has been published (Implementing acts, delegated acts,…) and processes are in place (conformity assessment,…).** |
| Annex I-section 1 – item (-a), (a) and (aa) | AGAINST | These requirements read "make available" which imply that they should be met for any commercial transactions on the product with digital elements: the placing on the market by the manufacturer or importer but also subsequent transactions carried out by distributors. As such these requirements appears as excessive.<br>For instance:<br>- **known exploitable vulnerability**. It is something constantly evolving. A vulnerability which is not exploitable or known at the placing on the market (by the manufacturer) may become exploitable in the course of a subsequent transaction (by a distributor) a few years later.<br>- **secure by default configuration**. This essential requirement applies to the manufacturer which shall make sure it is fulfilled. The manufacturer can ensure it is met when the product is placed on the market under his responsibility. Yet, in the case of subsequent transactions under the control of a distributor, the manufacturer can't ensure this requirement is met as the distributor may decide to change the configuration of the product with digital element so that it is not in a secure by default configuration. However, under the current wording, the manufacturer would remain liable in such situation.<br>In addition, the wording of "making available" used in these essential requirements is in contradiction with article 10(1) which explicitly states that essential requirements of Annex I-section 1 shall apply from the placing on the market.<br>**Therefore Eurosmart recommends to replace "made available" by "placed on the market"** |
| Annex I-section 1 – item (a) | AGAINST | The following essential requirements can't be met by some types of product with digital elements, and rather appears as a feature than an essential requirement:<br>- *"including the possibility to reset the product to its original state" in 3(a);*<br>**Therefore Eurosmart recommends removing this essential requirement** |
| Annex I-section 1 – item (aa) | AGAINST | The benefit of this requirement for the cybersecurity of product with digital element is unclear. This essential requirement rather appears as irrelevant.<br>In addition, it relates to internal design of product with digital elements, while the content of this annex should express essential requirements in a technology neutral manner in order not to impede innovation.<br>Therefore Eurosmart recommends removing this essential requirement |
| Annex I-section 1 – item (ab) | AGAINST | Eurosmart disagrees with this essential requirement. |

| Article/Recital | Eurosmart's feedback | Comments and proposals |
|---|---|---|
| Also see recital (32b) | | First of all, some products with digital elements may not be able to automatically install security update, especially because their connectivity depends on the user which may not always connect them (e.g. payment card)<br>Secondly, some products with digital element do not allow interaction with the user (e.g. they do not have screen or keyboard). Therefore, they may not be able to inform the user in any manner.<br>Therefore, Eurosmart recommends to remove the obligation for product with digital element to (1) support automatic update and (2) notify the user of available updates. |
| Annex I-section 1 – item (c) | SUPPORT | Eurosmart very much welcomes this addition |
| Annex I-section 1 – item (f) | SUPPORT | Eurosmart very much welcomes this addition |
| Annex I-section 1 – item (ka) | AGAINST | This requirements is explicitly forbidden for some type of products, for instance electronic passport, electronic identity documents, payment cards where:<br>- data should not be erased after issuance;<br>- the access to data is controlled by issuing authorities so that the user can't access on its own to the data;<br>**Therefore Eurosmart recommends removing this essential requirement** |
| Annex I-section 2 – item (2)<br>Also see recital (32b) | AGAINST | Eurosmart disagrees with this essential requirement.<br>Some products with digital elements may not be able to automatically install security update, especially because their connectivity depends on the user which may not always connect them (e.g. payment card).<br>**Therefore, Eurosmart recommends to remove the obligation for product with digital element to support automatic update.** |
| Annex I-section 2 – item (4) | AGAINST | Informing users about fixed vulnerabilities on the product with digital elements may raise substantial issues. Such information may be exploited by malicious entities to carry out cyber-attacks on products with digital elements that have not been fixed, or whose users have not applied mitigation measures. In such situations it is usually better to set up corrective measures without any further information to the users in order to limit the risks.<br>**Therefore, Eurosmart recommends to remove the obligation for manufacturer to inform users about fixed vulnerabilities on product with digital elements, and instead leave it to the CSIRT to decide whether or not user should be informed.** |
| Annex I-section 2 – item (8) | SUPPORT | "unless otherwise agreed between the parties in a business-to-business context"<br>Eurosmart very much welcomes this addition which allows existing business models where updates are charged to remain under the CRA. |

| Article/Recital | Eurosmart's feedback | Comments and proposals |
|---|---|---|
| Annex I-section 2 – item (8) | AGAINST | Eurosmart would like to highlight that the manufacturer can't ensure alone the "dissemination" of the security patch. It may be impossible in the case where the connectivity of the product with digital elements is made unavailable by the user (e.g. the user has not connected it to the Wi-Fi or to the internet). The dissemination of the security patch also relies on the actions and decisions of the user.<br>**Therefore, Eurosmart recommends replacing "dissemination" by "making available"** |
| Annex II<br>Item 8 | CLARIFICATION NEEDED | What is the meaning of "technical security support" |
| Annex II<br>Items 9(d) | AGAINST | Eurosmart highlights that such feature may not always be present in the products with digital elements. |
| Annex III<br>Class II<br>Item 12 and 13 | CLARIFICATION NEEDED | It seems these items should not be classified as class II but should rather be classified as highly critical product as they are intended for the use by essential entities of the type referred to in Article 3 of Directive (EU) 2022/2555<br><br>Clarification are needed |
| Annex VI<br>Module B-item 9<br>Module C-item 3.2<br>Module H-item 5.2 and item 6 | CLARIFICATION NEEDED | These provisions are not aligned with article 10(8) which states the following:<br>*"Manufacturers shall keep the technical documentation and the EU declaration of conformity at the disposal of the market surveillance authorities for at least ten years or the support period, **whichever is longer**, after the product with digital elements has been placed on the market."* |

# Annex II

# Comments on the EU Council's General Approach

| Article/Recital | Eurosmart's feedback | Comments and proposals |
|---|---|---|
| Recital (9a) | SUPPORT | Eurosmart welcomes this new recital which brings clarity to the scope of the regulation |
| Recital (9b) | SUPPORT | Eurosmart welcomes this new recital which brings clarity to the scope of the regulation |
| Recital (9c) | SUPPORT | Eurosmart welcomes this new recital which brings clarity to the scope of the regulation |
| Recital (10) | SUPPORT | Eurosmart very much welcomes the definition of commercial activity which is provided in the recital.<br><br>In addition, Eurosmart also fully shares the views of the Council whereby "The circumstances under which the product has been developed, or how the development has been financed should not be taken into account when determining the commercial or non-commercial nature of that activity". In particular, Eurosmart believes that the very nature of the actors which contributed to the development of a product, or the way it was developed shall not characterized the nature of the transaction that will occur. |
| Recital (10) | SUPPORT | Eurosmart very much welcomes the definition of free and open-source software. However, there is an editorial mistake in the text which should be fixed:<br><br>*"Free and open-source software is understood as free software that is openly shared and freely accessible, usable, ~~modified~~ modifiable to create new versions and redistributable, and which includes its source code and modified versions. Free and open-source software is developed, maintained, and distributed openly, including via online platforms."* |
| Recital (10) | SUPPORT | Eurosmart very much welcomes the clarification about free and open-source software as well as commercial activities |
| Recital (11a) | CLARIFICATION NEEDED | Eurosmart would like to highlight **that software update, security update or patch will most likely take the shape of a software which will be executed by the product with digital element. However, those should not be considered as a product with digital elements themselves.**<br><br>Therefore, Eurosmart recommends clarifying this aspect by a dedicated recital:<br><br>**"software updates, security updates or patches alone which are intended for products with digital elements are not product with digital elements."** |
| Recital (11a) | SUPPORT | Eurosmart very much welcomes the clarifications brought regarding the support of automatic update feature. |
| Recital (18) | AGAINST | Eurosmart believes that it **is key to alleviate the conformity tasks by mutualising as much as possible conformity tasks required by eIDAS and this proposal.** Doing so would alleviate the burden for industry and stakeholders thus decrease costs, which would foster the uptake of eIDAS and the wallet.<br><br>**Therefore, Eurosmart recommends keeping the text – second half of the recital which has been deleted.- <u>describing how to mutualise conformity tasks between eIDAS and this proposal.</u>** |
| Recital (18a) | AGAINST | Eurosmart very much welcomes the clarifications brought regarding the due diligence obligation.<br><br>However Eurosmart has concerns regarding the last sentence of this recital:<br><br>*"The vulnerability handling obligations in this Regulation, which the manufacturers have to comply with when placing a product with digital elements on the market and for the expected product lifetime, apply to products with digital elements in their entirety, including to all integrated components"* |

| Article/Recital | Eurosmart's feedback | Comments and proposals |
|---|---|---|
| | | Eurosmart believes this provision, should be clarified as it appears as misleading:<br>- First it should be clarified, that the vulnerability handling of the "integrated components" applies to the manufacturer of the integrated components and not the manufacturer of the product with digital elements which integrate them.<br>- Secondly, it shall be made clear that the vulnerability handling carried out by the manufacturer of a product with digital element integrating components may be different from the vulnerability handling carried out by the manufacturer of components. They may differ, as the impact of a vulnerability may be different.<br><br>**Therefore, Eurosmart recommends modifying the text as follows:**<br>**"The vulnerability handling obligations in this Regulation, which the manufacturers have to comply with when placing a product with digital elements (which may be a component integrated within a larger product with digital element) on the market and for the expected product lifetime, apply to products with digital elements in their entirety, ~~including to all integrated components~~"** |
| Recital (18a) | CLARIFICATION NEEDED | The meaning of this statement is confusing and should be clarified:<br>"The vulnerability handling obligations in this Regulation, which the manufacturers have to comply with when placing a product with digital elements on the market and for the expected product lifetime, apply to products with digital elements in their entirety, including to all integrated components."<br>Eurosmart recommends clarifying this statement |
| Recital (22) | SUPPORT | Eurosmart very much welcomes the clarifications brought regarding compliancy of products with essential requirements. |
| Recital (22a) | SUPPORT | Eurosmart very much welcomes the clarifications brought on whether a software update should be considered as a substantial modification of the product with digital elements or not. In particular, it is clarified that security update are not considered as a substantial modification. |
| Recital (25) | AGAINST | The example of secure element might not be relevant as secure element are now classified in annex IIIa. |
| Recital (27) | CLARIFICATION NEEDED | Eurosmart very much welcomes the clarification brought to the concept of "***core functionality***" and the composition rules.<br>However, Eurosmart believes some clarifications should be brought to the composition rules.<br>In the example, it should be clarified that firewalls, intrusion detection or prevention systems may be either (1) a product with digital elements (thus placed on the market) integrated within another product with digital elements, or (2) a component – not necessarily placed on the market as supplied internally - integrated within a product with digital elements. In both cases, firewalls, intrusion detection or prevention systems should be subject to mandatory third-party conformity assessment.<br>**Therefore, Eurosmart suggests amending the text as follows:**<br>**"[…] For example, Annex III to this Regulation lists products which are defined by their core functionality as firewalls, intrusion detection or prevention systems in class II. As a result, firewalls, intrusion detection or prevention systems are** |

| Article/Recital | Eurosmart's feedback | Comments and proposals |
|---|---|---|
| | | **subject to mandatory third-party conformity assessment. Firewalls, intrusion detection or prevention systems may be either (1) a product with digital elements (thus placed on the market) integrated within another product with digital elements, or (2) a component – not necessarily placed on the market as supplied internally - integrated within a product with digital elements. In both cases, firewalls, intrusion detection or prevention systems should be subject to mandatory third-party conformity assessment. This is not the case for other products not explicitly referred to in Annex III to this Regulation which may integrate a firewalls, intrusion detection or prevention systems. […]"** |
| Recital (30) | AGAINST | Eurosmart believes that a clear presumption of conformity with the essential requirements of Regulation (EU) 2023/1230 of the European Parliament and of the Council relating to cybersecurity aspects should be enacted in the regulation, in the same way as article 8(1) for the AI Act. It would alleviate the burden of manufacturer. This recital may indeed be useful but is clearly not sufficient. |
| Recital (32a) | AGAINST | *"as it is often the case with products with digital elements placed on the market by micro and small enterprises,"*<br><br>Eurosmart does not agree with the relation made between "micro and small enterprises" and "product with digital elements used only by a limited number of users or in less critical or sensitive environments". These two facts are not correlated and thus this link is misleading and false.<br><br>**Therefore, Eurosmart recommends removing this statement.** |
| Recital (32aa) | SUPPORT | Eurosmart very much welcomes this recital which clarifies that compliancy to standard may prevail in some cases even if it implies not to abide by all essential requirements. |
| Recital (45) | CLARIFICATION NEEDED | "This also applies to cases where a manufacturer chooses to not apply in whole or in part an applicable harmonised standard, common specification or European cybersecurity certification"<br><br>This sentence, within the context of the recital is misleading |
| Recital (46c) | SUPPORT | Eurosmart very much welcomes this initiative to leverage relevant EU funding programmes, the ECCC and NCC, as well as the European Digital innovation hubs to support manufacturers in the implementation of this regulation. |
| Recital (48a) | AGAINST | Eurosmart doesn't agree at all with this recital.<br><br>First, IT security laboratories accredited and notified under the EU CSA (regulation 2019/881) have already been assessed regarding their capacity to carry out security assessment and their skills and competencies are steadily monitored. Therefore, they should be exempted from assessment and notification under this regulation and should be automatically notified under this regulation.<br><br>In addition, Eurosmart would like to highlight that IT security laboratories established under the EU CSA (regulation 2019/881) will not be able to comply with the requirements enacted in article 39(4), 39(5) and 39(6) since the EU CSA provides for clear separation between bodies responsible for the assessment on one side, and bodies responsible for certification on the other side. By essence, the governance provided for in the EU CSA can't fit into the one considered by this regulation.<br><br>**Therefore, Eurosmart recommends to remove this recital and instead add a recital indicating that CAB established under the EU CSA (regulation 2019/881) should be exempted from assessment and notification under this regulation and should be automatically notified under this regulation.** |
| Recital (11a)<br><br>Recital (27aa) | CLARIFICATION NEEDED | These provisions still refer to the wording ***"intended use"***, ***"intended to be used"*** or ***"intended for the use" which*** may be confusing. It should be replaced by intended purpose as in the rest of the text. |

| Article/Recital | Eurosmart's feedback | Comments and proposals |
|---|---|---|
| Article 2(1) | | ***Recital (11a)***<br>***"[…] with digital elements intended to be used […]"***<br><br>***Recital (27aa)***<br>***"[…] is intended for the use […]"***<br>***"[…] products intended for the use […]"***<br><br>***article 2(1):***<br>***"This Regulation applies to products with digital elements whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network."*** |
| Article 2(4)<br>Second paragraph (deleted)<br><br>Also refer to recital (14) | CLARIFICATION NEEDED | Now that the second paragraph is deleted, the way the application of the CRA may be limited or excluded should be clarified. More precisely:<br>• Which legal vehicle should be used to do so (IA, DA, etc.)?<br>• Who is entitled to decide such exclusion or limitation? the EC? MS? The developer itself?<br>**Eurosmart recommends clarifying this aspect.** |
| Article 2(4a) | CLARIFICATION NEEDED | This provision is unclear and should be clarified:<br>(1) the components may indeed be supplied by the manufacturer of the product with digital elements. However, in some cases, it may also be directly supplied by the manufacturer of the components itself, under the responsibility of the manufacturer of the product with digital elements. This case is not reflected in the current wording.<br>**(2)** The meaning of "[...] are supplied by [...]" is unclear. Does it mean that only the transactions on the component between the manufacturer of the products with digital elements and its customer are excluded from the CRA? If so, does it mean that the placing on the market of the component (transaction between the manufacturer of the component and the manufacturer of the product with digital elements) is covered by the CRA? **Eurosmart believes that both the placing on the market and the making available on the market of the components should be excluded from the CRA, provided they are intended to replace identical components in a product with digital elements.**<br>Therefore, Eurosmart recommends modifying this provision as follows:<br>**"This Regulation does not apply to components that are exclusively manufactured as spare parts intended to replace identical components and are supplied by the manufacturer of the original product with digital elements or under its responsibility following the same development and production processes as the original product."** |

| Article/Recital | Eurosmart's feedback | Comments and proposals |
|---|---|---|
| Article 3(1) | CLARIFICATION NEEDED | It seems the definition also considers the case where the product with digital elements is placed on the market in several parts.<br><br>Does it means that in the case of a product with digital element having dependencies on an external software (e.g. Windows), windows is considered as part of the product with digital element? |
| Article 3(6)<br><br>Recital (7) | CLARIFICATION NEEDED | The meaning of computer code is unclear and should be further defined.<br><br>Data, when processed by another software or hardware could be understood by national authorities in the light of the definition provided for in article 3(6) as being a "computer code" (For example a word file, or a movie on a DVD, processed by a software to trigger some specific actions).<br><br>It seems it is not the intention of the text to also cover data whether formatted in machine-readable format or not. However, this ambiguity could lead to major divergence of implementation of this text within EU.<br><br>Therefore, Eurosmart believes a clarification should be brought in that regards to remove any ambiguity and risk of divergence of implementation with EU.<br><br>***Thus Eurosmart recommends adding the following text within recital (7):***<br><br>***"Data (personal or non personal) whether formatted in a machine readable language or not is not a software."*** |
| Article 3(38a) | SUPPORT | Eurosmart very much welcomes this new definition which is key for the implementation of Annex I – section 1 |
| Article 3(39)<br><br>Also refer to recital (19a) | AGAINST | The proposed definition of ***"actively exploited vulnerability"*** seems broader than the one proposed by the European Commission in its proposal, as now unsuccessful attempts are also included. This broader definition raises questions.<br><br>Only attempts for which the consequences are visible are likely to be noticed, meaning those that are successful. In contrast, unsuccessful attempts, without any consequences are very likely not to be noticed. Therefore, it seems very difficult for the manufacturer from a practical standpoint to establish and identify unsuccessful attempts of exploitation of vulnerabilities.<br><br>**Therefore, Eurosmart recommends to only include in the definition of "actively exploited vulnerability" successful attempts.** |
| Article 3(43) | SUPPORT | Eurosmart very much welcomes this definition which was missing. |
| Article 4(6) | SUPPORT | Eurosmart very much welcomes this clarification which ensures confidentiality of information which essence may be very sensitive. |
| Article 6(1a) | SUPPORT | Eurosmart very much welcomes this clarification as it provides for clear criteria for the classification of a product into Class I or Class II. These criteria will guide any further modifications of Annex III |
| Article 6(3)<br><br>Also refer to recital (63) | AGAINST | For the smooth implementation of the CRA and to ensure legal certainty the definitions of product categories connot be provided 6 months after the date of entry into force of this regulation. The definitions, together with product categories are absolutely needed by the industry so that it could adapt as soon as possible to the CRA, whose impacts will be substantial.<br><br>**Eurosmart recommends providing the definitions at the same time as the regulation, and also have them subject to the same scrutiny process as the regulation itself.** |
| Article 6a | AGAINST | Eurosmart recommends prioritizing the implementation of the CRA principles like implementation of Essential Cybersecurity Requirements on those product categories where the conformance mechanisms are not yet regular practice. Certification obligation in the CRA context for all high-end security products will complexify existing high-level evaluation processes. Several types of evaluations |

| Article/Recital | Eurosmart's feedback | Comments and proposals |
|---|---|---|
| Also refer to recital (27a) and (27aa) | | are already required for various sectors and have maintained products at the State-of-the-Art for years through the assessment of advanced and sector-specific security requirements. |
| Article 8(1) bullet (c) | CLARIFICATION NEEDED | The meaning of this statement is totally unclear. Clarification with regards to the obligation or possibility for the manufacturer should be brought. |
| Article 10(2a) | SUPPORT | Eurosmart very much welcomes this addition, which clarifies how to carry out the cybersecurity risks assessment, which is instrumental to comply with the provisions of the CRA.<br><br>In addition, this provision clarifies that requirements from Annex I section 1 point 3 which are non-applicable should be discarded from the cybersecurity risk assessment. |
| Article 10(6)<br><br>First paragraph | AGAINST | Pursuant to this proposed provision, the manufacturer of the product with digital element shall also ensure that the vulnerability on the components are handled in accordance with Annex I section 2.<br><br>Eurosmart would like to highlight that it may not always be possible. For instance, in the case where the component is an open source library, the manufacturer of the product with digital element is not in position to handle vulnerabilities in such components if the provider of the open source library does not (especially security update, but also identification of vulnerability,). In addition, as open-source libraries are likely to be out of the scope of the CRA, their providers will not be required to handle vulnerability in accordance with the CRA. Therefore, this proposed provision is excessive as it puts all the burden on the manufacturer of the product with digital elements while the component provider may not fall under the CRA. Finally, it shall be noted that vulnerability handling of the product with digital element will indeed take into account the components insofar as it is relevant for the product with digital element.<br><br>**Therefore, Eurosmart recommends removing the following wording:" ~~including its components~~"** |
| Article 10(6)<br><br>Second paragraph<br><br>Also refer to recital (33-a) | SUPPORT BUT WITH ADDITIONS | The expected product lifetime should indeed be determined in accordance with the criteria listed herein. However, other criteria which could also limit the expected product lifetime should also be considered, such as:<br><br>(1) the nature of the technology which may limit the possibility to provide security update over time. For instance, hardware based product may be harder to fix if a vulnerability directly stems from the hardware design of the product; or<br><br>(2) the nature of the conformity assessment and reviews of the security of the product with digital elements (Annex I – section 2 – point 3). If In-depth conformity assessment or reviews of the security of product are used (e.g. EU CSA security certification), a higher and deeper knowledge of the product with digital element and its design is provided, combined with a proactive identification of product impacted by vulnerabilities, which in turn is prone to spot any vulnerabilities.<br><br>**Therefore Eurosmart recommends adding the following criteria for the definition of the expected product lifetime:**<br><br>**(1) the nature of the technology which may limit the possibility to provide security update over time. For instance hardware based product may be harder to fix if a vulnerability directly stems from the hardware design of the product; or**<br><br>**(2) the nature of the conformity assessment and reviews of the security of the product with digital elements (Annex I – section 2 – point 3). If In-depth conformity assessment or reviews of the security of product are used (e.g. EU CSA security certification), a higher and deeper knowledge of the product with digital element and its design is** |

| Article/Recital | Eurosmart's feedback | Comments and proposals |
|---|---|---|
| | | **provided, combined with a proactive identification of product impacted by vulnerabilities, which in turn is prone to spot any vulnerabilities.** |
| Article 10(6)<br>Fourth paragraph | CLARIFICATION NEEDED | It should be clarified from when the security update should be made available for 10 years : **the placing on the market or the release of the security update?** |
| Article 10(6a) | SUPPORT | Eurosmart very much welcomes this provision. It may be very useful for manufacturers which may have placed on the market several versions of a software and that would like to alleviate the burden of security update preparation by only issuing security updates for the latest version |
| Article 10(12) | CLARIFICATION NEEDED | It should be clarified which of the essential requirements of Annex I – section 1 should be met from the placing on the market over the expected product lifetime (see dedicated comment on that point). Eurosmart recommends bringing clarification on that point. |
| Article 10(15) | CLARIFICATION NEEDED | The format of the information and instructions referred to in Annex II should be defined as soon as possible to provide visibility to industry, which will be substantially impacted by the CRA. Therefore, the definition of this format should not be postponed after the adoption of the text, but defined in the course of the adoption of the regulation.<br>**Eurosmart recommends defining in the regulation the format of the information and instructions referred to in Annex II, and not postponing it after the adoption of the regulation.** |
| Article 11<br>Also refer to recital (34) and (35) | AGAINST | The reporting obligations introduced in this article should be limited in time. Under the current version, they are perpetual, which is not acceptable for manufacturers. Manufacturers should not be required to abide by these obligations decades after the products with digital elements are not produced anymore.<br>**Therefore, Eurosmart recommends introducing a limitation in time for the reporting obligations.** |
| Article 11(1a)<br>Article 11(2a) | SUPPORT | Eurosmart very much welcomes this new process for the notification of actively exploited vulnerability. This process leaves more time to the manufacturer to collect and analyse information. |
| Article 11(2)<br>Article 11(2a)<br>Also refer to recital (34) | AGAINST | The provisions of these articles should only apply to significant incident. This approach would alleviate the burden for manufacturer while ensuring that only relevant and useful information about incidents is notified. A definition of "significant incidents" should also be included in article 3 to provide a legal basis for the manufacturer. |
| Article 11(2c)<br>Second paragraph<br>Sentence starting on line 5 | SUPPORT | Eurosmart very much welcomes this provisions, which may be useful in some situations. |

| Article/Recital | Eurosmart's feedback | Comments and proposals |
|---|---|---|
| Also refer to recital (35a) | | |
| Article 11(2c)<br>Second paragraph<br>7th line | SUPPORT BUT WITH ADDITIONS | This should also apply for notified information notified under paragraph 2a(a) i.e. incident having an impact on the security of the product with digital elements (and not only 1a(a) ). The provision should be updated accordingly. |
| Article 11(3) | | References to paragraphs 1(a) and 1(b) should be replaced by 1a(a) and 1a(b). |
| Article 11(4)<br><br><br><br>Also refer to recital (35) | AGAINST | Eurosmart has several concerns regarding the provision of this article.<br>First, **it may be difficult for manufacturer to inform users, as he may not know who the users are, especially when the products with digital elements are sold through distributors.**<br>In addition, informing users about an actively exploited vulnerability or an incident having an impact on the security of the product with digital elements may raise substantial issues. **It may put at risk industrial and/or trade secrets belonging to the manufacturer. Also such information may be exploited by malicious entities to carry out cyber-attacks on products with digital elements that have not been fixed, or whose users have not applied mitigation measures. In such situations it is usually better to set up corrective measures without any further information to the users in order to limit the risks.**<br>**Therefore, Eurosmart recommends to remove the obligation for manufacturer to inform users about an actively exploited vulnerability or an incident having an impact on the security of the product with digital elements, and instead leave it to the CSIRT to decide whether or not user should be informed.** |
| Article 13(6)<br>Second paragraph | CLARIFICATION NEEDED | The text reads the following:<br>*"[…] importers shall immediately inform the market surveillance authorities of the Member States in which they made the product with digital elements available on the market to that effect, [..]"*<br>However, as importer places products on the market, and does not make them available on the market, Eurosmart suggests changing the text accordingly as follows:<br>***"[…] importers shall immediately inform the market surveillance authorities of the Member States in which they ~~made~~ placed the product with digital elements ~~available~~ on the market to that effect, [..]"*** |
| Article 13(8) | CLARIFICATION NEEDED | For consistency reasons, the same additions should also be made for distributor in article 14(5) |
| Article 14(3) | CLARIFICATION NEEDED | Eurosmart very much welcomes this addition of "without undue delay" in the case of distributor. However, for consistency reasons, the same addition should also be made for importer in article 13(3) |
| Article 14(6) | CLARIFICATION NEEDED | Eurosmart very much welcomes this addition of "without undue delay" in the case of distributor. However, for consistency reasons, the same addition should also be made for importer in article 13(9) |
| Article 16<br>First paragraph | CLARIFICATION NEEDED | In accordance with the definition of manufacturer (article 3(18) ), a natural or legal persons placing a product with digital elements on the market under his or her name or trademark shall be considered a manufacturer for the purposes of this Regulation. |

| Article/Recital | Eurosmart's feedback | Comments and proposals |
|---|---|---|
| | | The content of the first paragraph shall be amended accordingly as follows:<br>**"A natural or legal person, other than the manufacturer, the importer or the distributor,that places a product with digital elements on the market under his or her name or trademark or carries out a substantial modification of the product with digital elements shall be considered a manufacturer for the purposes of this Regulation."** |
| Article 18(3)<br>Article 18(7)<br><br>Also refer to recital (41) | AGAINST | These articles are underpinned by the idea whereby (1) hENs should prevail over common specifications (common specification should be repealed where an hEN is published in the OJEU) and (2) common specifications should be seen as a last-resort option, when no hENs are available.<br>Eurosmart believes this approach of common specification is far too limitative. Common specifications may also be very useful to leverage existing industry or sector specific standards for which it has been demonstrated that they meet some or all of the essential requirements of Annex I. As such, common specification could support a quick implementation of the CRA, while limiting the impact on the industry.<br>Therefore Eurosmart recommends withdrawing article 18(7) and modifying article 18(3) so that IA establishing common specification could be adopted even if hEN are available or under preparation. |
| Article 18(5) | CLARIFICATION NEEDED | The nature of the "expert group" should be clarified as well as:<br>- the stakeholders that could join;<br>- the criteria to join<br>- the way to apply<br>- the mandate of the expert group |
| Article 18(9)<br><br>Also refer to recital (62) | AGAINST | The reference to the security certification level "substantial" or "high" should be maintained. Such security certification levels are commensurate with the requirements for conformity assessment for Class I and Class II, namely conformity assessment under the supervision of a third party.<br>**Therefore, Eurosmart recommends re introducing the reference to the security certification level "substantial" or "high".** |
| Article 22(1) | SUPPORT WITH ADDITIONS | Eurosmart also suggests allowing affixing the CE marking on the webpage referenced by the simplified EU declaration of conformity. |
| Article 23(2) | AGAINST | This obligation should be limited in time. Does it mean that this obligation is perpetual? Even after the product with digital element is not produced available on the market?<br>**Therefore, Eurosmart recommends reintroducing a limitation in time for this obligation.** |
| Article 24(2)<br>First paragraph | MISTAKE | For consistency, occurrences to European cybersecurity certification schemes should be removed, as such option is also proposed as a possibility in the following list. |

| Article/Recital | Eurosmart's feedback | Comments and proposals |
|---|---|---|
| Article 24(2)<br>Third bullet<br><br>Article 24(3)<br>Third bullet | AGAINST | The reference to the security certification level "substantial" or "high" should be added. Such security certification levels are commensurate with the requirements for conformity assessment for Class I and Class II, namely conformity assessment under the supervision of a third party.<br>**Therefore, Eurosmart recommends introducing the reference to the security certification level "substantial" or "high".** |
| Article 24(3aa)<br>First bullet | AGAINST | The reference to the security certification level "substantial" or "high" should be added. Such security certification levels are commensurate with the requirements for conformity assessment for and Class II (which is the fall-back option described in second bullet), namely conformity assessment under the supervision of a third party.<br>**Therefore, Eurosmart recommends introducing the reference to the security certification level "substantial" or "high".** |
| Article 24a(3)<br><br>Also refer to recital (46a) | AGAINST | Such provision creates distortion between SME and the others. If simplification in technical documentation is possible it should be available to all.<br>**Therefore Eurosmart recommends removing Article 24(a) and reintroducing the provision of article 24a(3) in article 23, and make it applicable to all, meaning not only SMEs.** |
| Article 26(3) | ADDITIONNAL ELEMENT | In such cases, in order to ensure fulfilment of all the applicable provisions, the body at stake shall be established under national laws of one MS and all its personnel shall be located in the EU. |
| Article 29(5)<br>Article 29(10) | ADDITIONNAL ELEMENT | **Eurosmart would like to highlight that these provisions regarding personnel (professional secrecy, professional integrity, free from pressures and inducements) as well as regarding confidentiality (article 52) can only be enforced and guaranteed provided each member of the personnel can be held liable if he doesn't abide by these rules.** Therefore, it implies that this regulation shall also apply in the country where the personnel at stake is located. If not, members of the personnel may not abide by these rules as they would not perceive any legal risks.<br>Yet, article 29 allows the personnel to be located outside the EU.<br>Therefore Eurosmart recommends adding the following requirement in article 29:<br>***"All personnel shall be located within EU."*** |
| Article 29(7) (C ) | SUPPORT | Eurosmart very much welcomes the addition of common specifications alongside harmonized standards as both may be used in the course of conformity assessment. |
| Article 35 | CLARIFICATION NEEDED | The consequences of the restriction, suspension or withdrawal of the notification of the notified body on the conformity assessment of a product with digital element should be further clarified:<br>- What happens to ongoing conformity assessments? Is it the responsibility of the notifying authority to assign them to another notified body?<br>- What happens to product with digital elements, which are monitored after initial conformity assessment by that notified body? Is it the responsibility of the notifying authority to assign them to another notified body? |

| Article/Recital | Eurosmart's feedback | Comments and proposals |
|---|---|---|
| | | **Eurosmart would like the co-legislators to clarify this point** |
| Article 37(4) | CLARIFICATION NEEDED | *"Certificate of conformity"* is not defined anywhere in the text, and it is unclear what it designates. As per our understanding, certificate of conformity designates any of the followings:<br>• EU type examination certificate (where module B is used);<br>• Approval decision (where module H is used)<br>***Eurosmart suggests adding a definition of "certificate of conformity" in article 3*** |
| Article 37(5)<br>Article 37(6) | CLARIFICATION NEEDED | Eurosmart would like clarifications regarding the consequences of the suspension or restriction of a certificate of conformity. What are the consequences for the product with digital elements? |
| Article 37a | SUPPORT | Eurosmart very much welcomes this addition which gives to manufacturers to possibility to appeal against the decision of a notified body. |
| Article 38(1)<br>Bullet (a ) | ADDITIONNAL ELEMENT | Eurosmart suggests using the wording "certificate of conformity" |
| Article 42 | AGAINST | Eurosmart recommends that this provision should be exercised within the limits of article 52 about confidentiality. |
| Article 44(4) | MODIFICATION | The reference to article 18(4) should be changed to Article 18(10) following changes made by the Council. |
| Article 49(3)<br><br>Also refer to recital (19) and (61) | SUPPORT WITH ADDITIONS | Eurosmart also recommends considering a second criteria for the sweeps, which is the type of conformity assessment procedure mostly used for a category of products with digital elements. As security certification pursuant to EU CSA brings a higher level of confidence - in particular because it is a white box approach, unlike conformity modules, categories of products with digital elements where module A, module B+C or module H are mostly used should also be given the priority by sweeps. |
| Article 53(3) | AGAINST | Pursuant to article 10(6), compliancy with Annex I – section 2 is only required for the expected product lifetime, while article 10(1) indicates that compliancy with Annex I – Section 1 is only required at the placing on the market. **Therefore, the requirement to comply with Annex I is limited in time.**<br>Therefore, this provision seems excessive and useless: "The non-compliance with the essential cybersecurity requirements laid down in Annex I should lead to an administrative fine […]". It is excessive as this wording ignores the limitation in time as enacted in article 10(6), and thus would mean that the essential requirements of Annex I would be mandated forever, even well after the expected product lifetime. It would create a major legal and financial risks for manufacturers which could even deter some of them to pursue their activities. In addition it is also useless as compliancy with Annex I is included in the provisions of article 10 which is explicitly quoted.<br>**Therefore Eurosmart recommends amending this provision as follows:**<br>**"The non-compliance with ~~the essential cybersecurity requirements laid down in Annex I and~~ the obligations set out in Articles 10 and 11 shall be subject to administrative fines of up to 15 000 000 EUR or, if the offender is an undertaking, up to 2.5 % of the its total worldwide annual turnover for the preceding financial year, whichever is higher."** |

| Article/Recital | Eurosmart's feedback | Comments and proposals |
|---|---|---|
| Article 55(3) | CLARIFICATION NEEDED | **This provision is unclear and seems in contradiction with article 57.**<br>Article 55(3) reads the following:<br>*"By way of derogation from paragraph 2, the obligations laid down in Article 11 shall apply to all products with digital elements within the scope of this Regulation that have been placed on the market **before** [XXX]"*<br>While article 57 reads the following:<br>*"However Article 11 shall apply **from** [24 months after the date of entry into force of this Regulation]."*<br>**Alignment is necessary** |
| Article 57 | SUPPORT WITH COMMENTS | Eurosmart very much welcomes this new timeframe for the application of this regulation. It leaves more time for stakeholders to bet ready for the implementation of the CRA. However, the implementation of the text should be carefully analysed.<br>Many companies, qualifying as "manufacturers", are suppliers of customers which also qualify as "manufacturers". This is the case where the customer (1) applies its own brand on the products with digital elements, (2) subcontracted the development, or (3) carried out substantial modification to the products with digital elements.<br>This element should be borne in mind when defining the timeline for the implementation of the text.<br>In that case, both the supplier and the customer should abide by the deadlines set forth in article 57, as both will place products with digital elements on the market (as they are both manufacturers). It entails that the supplier should be ready well ahead of time so that its customer could be ready on time.<br>This means that time enough should be left once all the supporting documentation has been published (Implementing acts, delegated acts,…) and processes are in place (conformity assessment,…) so that:<br>(1) the supplier could be ready and have compliant products with digital elements;<br>(2) the customer could sell all its stocks which does not comply;<br>(3) the customer could procure the new products with digital elements - which are compliant - to the supplier<br>If the time left to manage this transition is not enough, it may result in substantial disruption in supply chain, as well as financial loss.<br>Therefore Eurosmart recommends to let at least 3 years once all the supporting documentation has been published (Implementing acts, delegated acts,…) and processes are in place (conformity assessment,…). |
| Annex I<br>Section 1 | SUPPORT | Eurosmart very much welcomes the updated text in 3(aa) as it clarifies that the product with digital element shall not contain exploitable vulnerability at the placing on the market. |
| Annex I<br>Section 1 | CLARIFICATION NEEDED | The content of Annex I gathers several types of essential requirements which may be classified as follows:<br>- Essential requirements applicable for the design of the product with digital elements and before its placing on the market : 1; 3(h) and 3(i);<br>- Essential requirements applicable at the placing on the market of the product with digital elements : 3(a), 3(aa) and 3(aaa); |

| Article/Recital | Eurosmart's feedback | Comments and proposals |
|---|---|---|
| | | **Regarding the rest of the essential requirements ( 3(aaa), 3(b), 3(c ), 3(d), 3(e ), 3(f ), 3(g) ), Eurosmart recommends these essential requirements to be met at the placing on the market and not over the expected product lifetime.**<br>**According to article 10(12), it seems that these essential requirements should be met from the placing on the market of the product with digital elements over the expected product lifetime.**<br><br>Eurosmart considers clarifications should be brought on this point within Annex I. **In addition, for better readability and understanding, Eurosmart suggests reshaping the content of Annex I to clearly distinguish the different types of essential requirements:**<br>- **those applicable for the design of the product with digital elements and before its placing on the market;**<br>- **those applicable at the placing on the market;**<br>- **those applicable from the placing on the market over the expected product lifetime;** |
| Annex I<br>Section 1 | AGAINST | The following essential requirements can't be met by some types of product with digital elements, and rather appears as a feature than an essential requirement:<br>- *"including the possibility to reset the product to its original state" in 3(a);*<br>- *"including a default setting that security updates be installed automatically" in 3(a);*<br>- *"with a clear and easy- to-use opt-out mechanism." In 3(a);*<br>- *"set as a default setting – which can be switched off – that security updates are installed automatically on products with digital elements if not installed within a certain timeframe" in 3(aaa);*<br>- *"through automatic updates by default, but with a clear and easy-to-use opt-out mechanism, and where applicable through the notification of available updates to users, and the option to temporarily postpone them" in 3(k);*<br>- *provide security related information by recording and/or monitoring relevant internal activity, including the access to or modification of data, services or functions" in 3(j)*<br><br>**Therefore, Eurosmart suggests to either remove them or to keep them and indicate that they are optional features.** |
| Annex I<br>Section 1<br>3(a) : "including the possibility to reset the product to its original state"<br>3(l) | AGAINST | These requirements are explicitly forbidden for some type of products, for instance electronic passport, electronic identity documents, payment cards where<br>- *data should not be modified nor erased after issuance;*<br>- *configuration of the product with digital elements should not be modified by the holder as it is the responsibility of the issuer to define and set it;*<br>- *the access to data is controlled by issuing authorities so that the transfer can't be organized by the user;*<br>**Therefore Eurosmart recommends removing these two essential requirements** |

| Article/Recital | Eurosmart's feedback | Comments and proposals |
|---|---|---|
| Annex I<br>Section 1<br>3(g) | CLARIFICATION NEEDED | The meaning of this essential requirement is unclear |
| Annex I<br>Section 2(4) | SUPPORT | Eurosmart very much welcomes the addition made by the council, which acknowledges that public disclosure of vulnerabilities may be risky.<br>This provision should be updated to allow the manufacturer not to publish at all the vulnerability with the consent of the CSIRT or the market supervision authority. Eurosmart believes that the same approach should also be applied in article 11(4), and information to users in case of "actively exploited vulnerability" or "incident having an impact on the security of the product with digital element" should not be the rule, and it shall be possible not to inform users in such cases (upon CSIRT agreement). |
| Annex I<br>Section 2(8) | AGAINST | Eurosmart would like to highlight that the manufacturer can't ensure alone the "dissemination" of the security patch. It may be impossible in the case where the connectivity of the product with digital elements is made unavailable by the user (e.g. the user has not connected it to the Wi-Fi or to the internet). The dissemination of the security patch also relies on the actions and decisions of the user.<br>**Therefore, Eurosmart recommends replacing "dissemination" by "making available"** |
| Annex II<br>Item 8 | CLARIFICATION NEEDED | What is the meaning of "technical security support"? |
| Annex II<br>Items 9(d) and 9(e) | AGAINST | Eurosmart highlights that such features may not always be present in the products with digital elements. |
| Annex III | SUPPORT | Eurosmart welcomes the clarifications brought to the content of this annex, where the categories of products with digital elements are much clearer. |
| Annex III | AGAINST | Eurosmart also notes that several categories of products with digital elements have been removed from Class I and Class II (IACS, industrial IoT, ASIC, browsers…).<br>Eurosmart recommends reintroducing them into the classification. |
| Annex IIIa<br>Item 3a | AGAINST | Eurosmart recommends reconsidering the mandatory certification to comply with CRA's essential requirements, prioritising the implementation of the CRA principles like implementation of Essential cybersecurity requirements on product categories where the conformance mechanisms are not yet regular practice |
| Annex V<br>Item 4 | MODIFICATION | The references to articles should be updated following changes made by the Council. |

## About us

Eurosmart, the Voice of the Digital Security Industry, is a **European non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com @Eurosmart_EU @Eurosmart

Square de Meeûs 35 | 1000 Brussels | Belgium
Tel +32 2 895 36 56 | mail Contact@eurosmart.com