Council of the European Union
General Secretariat

Interinstitutional files:
2022/0272 (COD)

Brussels, 25 January 2023

WK 843/2023 INIT

LIMITE

CYBER
JAI
DATAPROTECT
TELECOM
MI
CSC
CSCI
CODEC

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From: To:	General Secretariat of the Council Delegations
N° prev. doc.:	5308/23 15037/1/2022 REV 1 12429/2022 ADD 1-6
Subject:	Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020: delegations' comments on Block 2

Delegations will find attached comments by the BE, CZ, DK, DE, ES, FR, IT, LV, HU, NL and FI delegations on the above mentioned legislative proposal.

Table of Contents

BELGIUM 2
CZECH REPUBLIC 9
DENMARK 10
GERMANY 19
FRANCE 27
SPAIN 41
ITALY 48
LATVIA 55
HUNGARY 68
NETHERLANDS 71
FINLAND 75

BELGIUM

Belgian Written Comments on "Block 2" of the Cyber Resilience Act (requirements)		
	Comments	**Amendment suggestions**
Chapter II – Obligations of economic operators	Products with digital elements include very diverse types of products. The obligations that the CRA imposes on manufacturers of such products should be **proportionate to the risk** to which they expose users (but **without that the security of users be adversely affected).** **As a result, requirements might need to be calibrated more strict for categories of higher criticality**, instead of using categories only to determine the conformity assessment procedure. We do not want manufacturers of lower-risk products to be required to take exactly the same safety measures in the design as manufacturers of high-risk products. However, at present, there are **no standards or guidance on the risk analyses** required to determine this proportionality. It is therefore important to insist that manufacturers clearly communicate to users the level of ambition they choose for the security of their products.	See under Art. 10

Article 10 - Obligations of manufacturers	The **5-year or shorter lifecycle cap** for the compulsory handling of vulnerabilities under Art. 10(6) **does not seem appropriate.** For some products this will be too long to be a proportionate request, yet for others it will be too short. This would leave millions of connected products with lifecycles longer than 5 years open to attack, or it would encourage both buyers and distributors to discard products before the end of their expected lifespan. This would go against sustainable We suggest an alternative, more risk-based approach, as follows: 1. It is **left to the manufacturer to commit** to a minimum end-date of his support on the condition that: a. this commitment is **binding** on them b. the date is reasonable and proportionate to the type of product and its lifecycle c. this date is **clearly indicated on the product notice AND packaging**, so that users are duly informed and can choose to buy a product taking the length of the support into account, (this could support competition). 2. No maximum duration is imposed (which could support competition in this field) 3. We are open to an **obligated minimal length of support**, to avoid a race to the bottom, yet this date should be **reasonable, calibrated and flexible**.	Art.10(6): When placing a product with digital elements on the market, and **until at least a final date that is reasonable and proportionate to the type of product and its lifecycle ~~for the expected product lifetime or for a period of five years from the placing of the product on the market, whichever is shorter~~**, manufacturers shall ensure that vulnerabilities of that product are handled effectively and in accordance with the essential requirements set out in Section 2 of Annex I. **This final date shall be clearly and understandably indicated on the product or its packaging** Art.10**(10a): Manufacturers shall ensure that the products with digital elements or their packaging clearly and understandably indicate the end date, including at least the month and year, until which the manufacturer will at least ensure the handling of vulnerabilities in accordance with the essential requirements set out in Section 2 of Annex I.**

Article 11 - Reporting obligations of manufacturers	**The CRA should follow the logic of NIS2 for the notification of incidents and vulnerabilities**, i.e. that they should be reported to national authorities first, rather than to ENISA, as foreseen under Art. 11 (1) and (2). Although a single European point of contact has advantages for manufacturers, we believe that **this mechanism could be a slowing factor** in mitigating incidents. Moreover, the text provides for the possibility that ENISA itself decides not to transmit certain information received. This **goes against the logic of NIS-2**, according to which notifications, in particular of incidents, are always forwarded to a national authority, which then forwards them to ENISA. Nevertheless, if a central EU notification point is necessary, it would be preferable, for example, to set up an automatic platform, managed by ENISA, on which manufacturers could report incidents or vulnerabilities, which would then be automatically and fully transmitted to the competent national authorities and stored in a central register. In addition, we should **avoid duplication of incident reporting obligations** between the CRA and NIS2. CRA notification requirements should be better aligned with NIS2 to simplify the actual reporting of incidents and avoid legal discussions on whether or not an incident should be reported under NIS2 or under the CRA.	Art. 11 (1) and (2) should **be amended so that incidents and vulnerabilities are reported to national authorities first**, rather than to ENISA. More generally, notification requirements under the CRA should be **better aligned with NIS2.**

Article 13 - Obligations of importers	See justification under Article 10	Art.13**(5a): Importers shall ensure that the products with digital elements or their packaging clearly and understandably indicate the end date, including at least the month and year, until which the manufacturer will at least ensure the handling of vulnerabilities in accordance with the essential requirements set out in Section 2 of Annex I.**
Article 14 - Obligations of distributors	See justification under Art. 10 - We suggesting adding the requirement to display the end support date clearly on the packaging of the product:	Art.14(2)(b) the manufacturer and the importer have complied with the obligations set out respectively in Articles 10(10), **10(10a),** 10(11) and 13(4).
ANNEX I Security requirements & Vulnerability handling requirements	General comment: Annex I-1(1) states manufacturers should "ensure an appropriate level of cybersecurity" for products in relation to the risks envisaged. This requirement may wrongly give users the impression that products complying with the CRA are completely safe (offering a kind of "cybersecurity guarantee"). However, we know that in practice new vulnerabilities can always be discovered and that users can sometimes use products in a dangerous way. This is why we would like to stress the importance of monitoring and dealing with vulnerabilities, including the proposal to foresee the automatic installation of security updates by default. Ensuring an automatic installation of security updates by default:	- Annex I,1 (3)a: be delivered with a secure by default configuration, including the possibility to reset the product to its original state**, and including a default setting that security patches or updates be installed automatically according to requirements in Annex I,2 (9) and Annex II,(8a)**; - Annex I,1 (3)k: ensure that vulnerabilities can be addressed through security updates, including**~~, where applicable,~~** through automatic updates **by default, but with a clearly indicated opt-out mechanism, and through** the notification of available updates to users, **and the option to temporarily postpone them**. - Annex I,2 **(9): set as a default setting – which can be switched off – that security patches updates are installed automatically on products with digital elements if not installed within a certain timeframe;**

	Almost 80% of cyberattacks exploit vulnerabilities that were already known for two years or more, and for which security patches were available. Users simply did not install the available updates, either because they are unaware or have little incentive, time, or knowledge to do so. In order to solve this problem, we believe that manufacturers of products with digital elements should be required to: 1. provide security updates, but also establish **a default setting that security updates are installed automatically;** this default setting will contribute to placing products on the market **in their most secure state** 2. yet**,** since we do not wish that this default setting could disrupt critical or industrial environments, the default setting must be able to be easily turned off, 3. **And manufacturers should provide very clear instructions** with the product on how to turn off this default setting – **And they should clearly indicate, on the product or on its packaging, of the final date** (month and year) until which security updates will be provided for, so that buyers are informed.	
		- Annex II (8): the type of technical security support offered by the manufacturer and until when it will be provided, at the very least until when users can expect to receive security updates; **this earliest end date of support should also be clearly indicated on the product or its packaging;** - Annex II (**8a): clearly understandable instructions on how the default setting of automatically installed updates, as required by Annex I,2(9) can be turned off;**

Recitals	In line with our suggested amendments to art. 10, 13 & 14, we suggest adding two new recitals after current Recital 11.	**Recital (11a) Many cyberattacks exploit vulnerabilities that are known, often already for several years and for which patches exists. Findings show that security updates are not regularly applied by average users. This situation creates the possibility of millions of unpatched and thereby vulnerable products, which poses a threat to the entire connected digital society. Manufacturers should therefore introduce into their products with digital elements a default setting that security updates are installed automatically, especially if the user does not install them within a certain timeframe. This obligation should only apply for security updates, not functionality updates, and users should always be informed that an update will be installed, with the possibility for them to postpone the update, though not indefinitely. The product should also come with clear instructions on how this default setting can be turned off, when users, in particular expert users, would wish to install updates in a more controlled procedure, so that such updates would not interfere with operations in critical environments.** **Recital (11b) The end date, including month and year, until which manufacturers will at least keep providing security updates, should also be clearly indicated on the product or its**

		packaging, so as to allow consumers clear knowledge until when their product can be relied upon to remain updated.

CZECH REPUBLIC

CZ comments on block 2 of the Cyber Resilience Act proposal

General comment on obligations of economic operators

As the implementation of the CRA will require the allocation of additional capacities and financial resources from economic operators, we advocate for CRA measures to be proportionate and implementable for the various group of economic operators, especially for **SMEs and start-ups**. For this same reason, we encourage timely adoption of harmonized standards.

Art. 11, para. 1

Irrespective of who is the recipient of the notifications, there are potential security risks that come with reporting of actively exploited vulnerabilities because these vulnerabilities would be reported without being mitigated first. Therefore, reporting of such vulnerabilities and disseminating information about them must have a clear added value and be done as securely as possible. In the proposal, it is not foreseen that ENISA might act on these notifications. Its role is limited to being an intermediary between reporting manufacturers and national CSIRTs. Therefore, should ENISA receive and pass on these fairly sensitive notifications, the benefits of adding this intermediary role must outweigh the risks involved. Thus far, we are not convinced that this is the case. We would welcome to hear ENISA's view on this matter.

Art. 10 para. 4

We are of the opinion that it should be specified in a corresponding recital how a manufacturer perform its due diligence when integrating components sourced from third parties in products with digital elements. This recital should also specify what "compromise" means in the context of para. 4 as it is not clear.

Art. 10 para. 6

We believe that the period for which the manufacturer will ensure that the vulnerabilities of the product are handled effectively and in accordance with the essential requirements set out in section 2 of Annex I should be set clearly and indicated visibly so that it properly servers the purpose of informing the user about security support he/she can expect. Also, we are of the opinion that the "product lifetime" concept should be specified/defined either in the corresponding recital or in the list of definitions in the Art. 3 of the Proposal.

DENMARK

DK comments – Proposal for a Cyber Resilience Act (COM(2022) 454)

We appreciate the considerable work on the proposal on horizontal cyber security requirements for products with digital elements thus far. The proposal has moved it in the right direction. We see a few outstanding issues regarding the chapters discussed under the Czech Presidency, and several more that have yet to be examined.

BLOCK I

Article 2

As a general comment, we find that there is still a need further clarity regarding scope; in particular, which products and services the Regulation will cover.

While recital 9 has been improved, there are still many unanswered questions in relation to open-source software, remote data processing and other digital solutions, which merits further examination. For example, we find the wording previously added to rec. 9 regarding websites is confusing and should be deleted:

(9) "... ~~In addition, websites would not constitute remote data processing solutions of web browsers since they are not developed under the responsibility of a browser manufacturer and as the absence of any individual website would not prevent a browser from performing its functions~~…"

Proposal for a new recital 13a

Regulation (EU) No 167/2013 establishes the requirements for the approval and market surveillance of agricultural and forestry vehicles. Vehicles with digital elements to which that Regulation applies are also subject to the CRA.

The CRA includes references to legislation where vehicles are either included or exempted from the scope of application. This includes the reference to Regulation (EU) 2019/2144 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users and to the Machinery Regulation, recital 30 and Article 9.

We would like to get a clarification on whether two- or three-wheel vehicles and quadricycles are also subject to the CRA. If these vehicles are indeed subject to the regulation, we suggest including Regulation 168/2013 in a new recital.
There is a need for further clarification in the recitals to avoid misunderstandings regarding which vehicles with digital elements are subject to this proposed Regulation.

We suggest the following clarifying Recital 13 a on the scope of application as regards the above mentioned vehicles:

(13a) Regulation (EU) No 167/2013 of the European Parliament and of the Council establishes the requirements for the approval and market surveillance of agricultural and forestry vehicles and Regulation (EU) No 168/2013 of the European Parliament and of the Council establishes the requirements for the approval and market surveillance of two- or three-wheel vehicles and quadricycles. Vehicles to which either of those Regulations apply with digital elements are subject to this Regulation.

Products made available by public authorities

We would like to recall our written comments of 14 December 2022 suggesting changes to recital 10, specifying the distinction between commercial products and products made available by public authorities. For convenience, they are repeated below:

(10) In order not to hamper innovation or research, free and open-source software developed or supplied outside the course of a commercial activity should not be covered by this Regulation. This is in particular the case for software, including its source code and modified versions, that is openly shared and freely accessible, usable, modifiable and redistributable. In the context of software, a commercial activity might be characterized not only by charging a price for a product, but also by charging a price for technical support services, by providing a software platform through which the manufacturer monetises other services, or by the use of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software. **Products [and Services] made available by public authorities as part of their responsibilities can only be considered of a commercial nature in cases where a price is charged for the use of that product or service that exceeds what may be considered reasonable to cover operational costs directly related to the functioning of the product or service in question.**

BLOCK II

Article 5 & 6

Standardisation

The act aims to set the same essential cybersecurity requirements for all products with digital elements. At the same time, the regulation needs to replace a number of other cybersecurity rules, i.e., in the product safety and radio equipment directives. As a result, the requirements for some products are increasing, which is why the three levels ("normal" and critical class I and II) are introduced in annex III.

We think it is important to reflect on this at the current stage, because the traditional way of dealing with more critical products would be to increase requirements as well as level of scrutiny of evaluations depending on the level of criticality – as for example done through the CSA levels of basic, substantial and high.

The risk is that we during the negotiations will not deal with the challenges inherent in the above, and they instead will surface later when the standardisation bodies set about implementing the legislation. This may very well result in three levels of standards being introduced, in which case we might as well streamline the CRA with the CSA from the start. There is also a risk that the standardisation organisations will end up creating one standard per product type listed in annex III, which would exacerbate already existing problems of a patchwork of standards, making it difficult, inefficient and expensive for both companies and authorities to manage. This would go against the very aim of this horizontal regulation.

If the current horizontal essential requirements are to be maintained, **we need input from the standardisation organisations on whether a single standard can fully encompass all products**; from trivial to very critical ones, in a way that provides meaningful protection, and which can be understood by manufacturers.

Ideally, our preference is to have a regulation with one basic level of security across all products, referring to one standard governing the practical implementation.

To ensure that the requirements are meaningful and practically implementable, we urge the Presidency to consider **setting up a workshop** where experts on standardisation, e.g., CEN-CENELEC, could elaborate on the concerns raised and to discuss how to manage the width of the CRA's scope in practice by standards. In this workshop, experiences from the RED-standardisation work could also be shared.

Delegated powers to the Commission (art. 6(3 & 5))

We are concerned that the chosen approach is not sufficiently clear and transparent. With a reservation for further scrutiny, we propose at a minimum to change the type of acts from delegated to implementing acts.

Further, we look forward to a thorough examination of the listed products in annex III, and to understand further, how they have been assessed against the requirements listed in article 6.

Article 10

We find that the 5 years limitation in art. 10(6) runs counter to both the purposes of the CRA and the goals of the European Green Deal.

Many products have (or should have) lifespans exceeding 5 years and, in a world where cybersecurity is an ever-increasing concern, this limit could set an unintentional and unwanted expiration date on such products.

Many users, and in particularly consumers, would continue to use such products past such a limit – out of necessity/lack of alternatives or in ignorance of the risks – subjecting themselves and others to danger and thereby, undermining the aims of this regulation. Other users would opt to discard such products, which could have otherwise continued to fulfil their function for many more years. Such a waste of resources conflicts with our common goals of sustainability.

Therefore, we suggest deleting this 5-year limitation, leaving 'expected product lifetime' as the sole factor:

Article 10(6):

> When placing a product with digital elements on the market, and for the expected product lifetime ~~or for a period of five years from the placing of the product on the market, whichever is shorter~~, manufacturers shall ensure that vulnerabilities of that product are handled effectively and in accordance with the essential requirements set out in Section 2 of Annex I.

Similar can be deleted in Articles 10(12) and 23(2).

Furthermore, we suggest exploring whether it is possible to add useful references about expected lifetime assessment from other relevant legislation, e.g. Eco-design legislation.

Article 11

We are not in favour of the extended mandate and authority ENISA receives with the Regulation.

Particularly, we are concerned whether ENISA has the capacity to confidently handle the data from manufacturers regarding vulnerabilities, incidents etc., especially if the data is critical or related to critical products. We believe that placing information about active vulnerabilities and incidents from manufacturers in 27 MS in the same database is a serious security risk. Such database will naturally become a primary target for malicious actors. Thus, we are not in favour of the proposed notification model.

We would suggest changing the model, so the manufacturers report directly to the national CSIRT, who can then share the notification to other MS through the CSIRT-network and ENISA in a timely manner. It is our opinion that ENISA should not receive notifications of vulnerabilities before Member States. We support the reporting mechanism established in NIS2, where notifications are directed at CSIRTs. In NIS2 we have already built a strong collaboration structure that has the necessary infrastructure for such collaboration. Moreover, every national CSIRT is manned 24/7, is (or will be) fully operational when CRA will be in force, and has experience with handling incidents and vulnerabilities. This has required many investments at the national level. These capacities are also not the same, as the capacities ENISA are developing in regards to the vulnerability database in NIS2. There is a big difference between being responsible for the creation and update of a database, where most of the work is not time sensitive and would not require further action from ENISA, than responding to incident and vulnerability notification, where there is a great deal of time sensitivity, and a need to take action.

In practice, we could follow the jurisdiction model of NIS2, where the producer should notify the MS national CSIRT in the MS in which its HQ is placed. If the producer does not have an HQ within the EU, the reporting could be made to the MS national CSIRT in the MS in which its authorised representatives are located. The national CSIRT could then have the task to share this information in the CSIRT network, so that all national CSIRT are made aware of incidents and exploited vulnerabilities in products that might be present on their national markets. This would of course necessitate that the information channels for sharing information in the CSIRT-network are very secure.

Specifically regarding 11(3), it is difficult for us to see how such information might be relevant for CyCLONe. The information would be more relevant for the CSIRT-network in the case where they are activated due to the exploitation of a vulnerability leading to a large scale incident. The national CSIRT could then inform the national CyCLONe officer.

We would like to know the Commission's considerations behind the proposed model for reporting obligations, especially the considerations behind not utilising the reporting mechanism established with NIS2.

We have concerns that ENISA's role will operationalise ENISA that does not – and should not – have an operational role, which was very clear during the negotiations of ENISA's mandate in the Cyber Security Act. It is our understanding that ENISA will have to analyse and evaluate the data, which ENISA receives in order to e.g. produce biennial technical reporting on emerging trends regarding cybersecurity risk in products, de facto making ENISA operative. Moreover, ENISA should cf. recital 18 propose joint activities or coordinated control actions to be conducted by market surveillance authorities based on indications or information regarding potential non-compliance with the regulation. We fail to see how ENISA should refrain from using the empirical data gathered through notifications when proposing joint activities or simultaneous coordinated control actions, adding to the fact that ENISA indeed will have an operative function with this regulation. We are sceptical of whether ENISA has the resources to be operative and carry out the tasks mentioned above sufficiently.

Additionally, we continue to question why the reporting obligations of manufacturers are limited to “actively exploited” vulnerabilities. We find it more appropriate to include “all known” vulnerabilities in the reporting, provided that a patch to address them is available. In this context, it may then also be advisable to introduce a ‘de minimis’ rule.

Article 15 & 16 + recitals 22-24 (cf. art. 3 (24 & 31))

The concept of "significant modification" is very important in the context of these articles. With the current definitions in the proposal, it is unclear to us, in what cases the obligations of the manufacturer apply to other actors, and when a new conformity assessment is needed. This is particularly due to the use of the term "intended use" in the definition of "substantial modification" in article 3(31) "Intended use" is not defined in this act, however "intended purpose" is in article 3(24) To ensure clarity, we would suggest using the term "intended purpose" rather than intended use. The same change would be necessary throughout recital 22, where the reference to "function, type or performance" leads to ambiguity regarding when software updates necessitate a new conformity assessment.

In accordance with the above, we recommend the following amendment:

Article 3(31):

> 'substantial modification' means a change to the product with digital elements following its placing on the market, which affects the compliance of the product with digital elements with the essential requirements set out in Section 1 of Annex I or results in a modification to the intended ~~use~~ **purpose** for which the product with digital elements has been assessed.
>
> *Recital 22:*
>
> "…For example, software updates or repairs could be assimilated to maintenance operations provided that they do not modify a product already placed on the market in such a way that compliance with the applicable requirements may be affected, or that the intended ~~use~~ **purpose** for which the product has been assessed may be changed. As is the case for physical repairs or modifications, a product with digital elements should be considered as substantially modified by a software change where the software update modifies the ~~original~~ intended **purpose** ~~functions, type or performance~~ of the product and these changes were not foreseen in the initial risk assessment, or the nature of the hazard has changed or the level of risk has increased because of the software update.

Annex I

Point 1(2) in Annex I states, "*products shall be delivered without any known exploitable vulnerabilities*". The Commission confirmed in the meeting on 18 January that this is an absolute requirement, not subject to the risk assessment referred to in point 1(3).

We find that this could lead to very high costs for manufacturers and endangers the proportionality of the proposal. All vulnerabilities are potentially (or may become) exploitable. What matters is the level of risk and potential harm these vulnerabilities pose. **We therefore recommend modifying this requirement and subjecting it to the risk assessment in 1(3).**

The term "*delivered*", which is used in both point 1(2) and point 1(3) does not seem appropriate to use in this context and may cause confusion. A product can be considered *delivered* when a customer receives it. However, the manufacturer, importer or distributor rarely maintain complete control of a product for the entire time until it can be considered delivered. As vulnerabilities are frequently discovered, it is not reasonable to require these economic operators to prevent delivery when a product has left their reach – e.g., while being delivered by a shipping company, stored in an intermediary's warehouse, store etc. **Hence, we suggest the term "delivered" be replaced with "placed on the market".**

In accordance with the above, we recommend the following amendment:

1. SECURITY REQUIREMENTS RELATING TO THE PROPERTIES OF PRODUCTS WITH DIGITAL ELEMENTS

   (1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks;

   ~~**(2) Products with digital elements shall be delivered without any known exploitable vulnerabilities;**~~

   (3) On the basis of the risk assessment referred to in Article 10(2) and where applicable, products with digital elements shall:

   (aa) be placed on the market without any known vulnerabilities, which pose a significant cybersecurity threat through its intended use;

   (a) be ~~**delivered**~~ **placed on the market** with a secure by default configuration, including the possibility to reset the product to its original state; (…)

Regarding point 1(3)(e), we note the answers given by the Commission in the HWPCI meeting on 18 January. However, we remain unconvinced that the inclusion of a data minimisation requirement in the CRA is necessary or appropriate. While we are strong proponents of data protection and fundamental rights, we find that: (1) neither are directly relevant to cybersecurity and, (2) both are regulated adequately and more appropriately elsewhere, such as the GDPR, ePrivacy, directive on trade secrets, AI Regulation and the Data Act.

Further, we find the inclusion in the CRA could potentially directly oppose the objectives of the Data Act and the EU vision for the data economy. To horisontally limit processing of non-personal data to only the intended use of the product, in all products with digital elements on the market, would have significant implications for the ability of European companies to innovate and compete globally. From a legal point of view, it would also be ill advised to prejudice the outcome of ongoing negotiations on the Data Act and ePrivacy Regulation.

Consequently, we propose the complete deletion of 1(3)(e) from Annex I, section 1.

As we have noted before, we would recommend changing the wording to "without **undue** delay" in point 2(2) & 2(8). In many cases, some delays cannot be avoided, e.g., due to resource constraints, force majeure, or other events.

Annex II

The Software Bill of Materials (SBOM) mentioned in point 2(6) may in the wrong hands also be a list of potential vulnerabilities for malicious use. We understand from the answers given by the Commission in the most recent HWPCI meeting on 18 January that the SBOM is only meant to be shared with the market surveillance authorities upon their request. However, this is not consistent with the current content of the annexes.

To ensure that the intended objectives are accurately reflected in the proposal, we suggest deleting point 6 of annex II.

GERMANY

GER comments on Block 2 CRA
(Art. 5 and Art. 10-17, Annexes I and II, including essential requirements and reporting obligations), (Recitals: 6, 19, 20, 22-24, 32-37, 42)

Recital

(20) Products with digital elements should bear the CE marking to indicate their conformity with this Regulation so that they can move freely within the internal market. Member States should not create unjustified obstacles to the placing on the market of products with digital elements that comply with the requirements laid down in this Regulation and bear the CE marking.

Commented [DN1]: This differentiation between different classes of products (as defined in Annexes) is neither visible nor plausible to consumers. This could be renderd more transparent and recognisable for users by adding labelling to the CE mark with a consumer focus.

(35) Manufacturers should also report to ENISA any incident having an impact on the security of the product with digital elements. Notwithstanding the incident reporting obligations in Directive [Directive XXX/XXXX (NIS2)] for essential and important entities, it is crucial for ENISA, the single points of contact designated by the Member States in accordance with Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] and the market surveillance authorities to receive information from the manufacturers of products with digital elements allowing them to assess the security of these products. In order to ensure that users can react quickly to incidents having an impact on the security of their products with digital elements, manufacturers should also inform their users about any such incident and, where applicable, about any corrective measures that the users can deploy to mitigate the impact of the incident, for example by publishing relevant information on their websites or, where the manufacturer is able to contact the users and where justified by the risks, by reaching out to the users directly.

Commented [DN2]: In our understanding this is also partly adressed with Art. 12 (2) NIS2.

Article 10

Obligations of manufacturers

4. For the purposes of complying with the obligation laid down in paragraph 1, manufacturers shall exercise due diligence when integrating components sourced from third parties in products with digital elements. They shall ensure in a reasonable manner that such components do not compromise the security of the product with digital elements.

Commented [DN3]: This could be otherwise lead to improper obligation with a view on complex components used by the manufacturer.

6. When placing a product with digital elements on the market, and for the expected product lifetime or for a period of five years from the placing of the product on the market, whichever is shorter, manufacturers shall ensure that vulnerabilities of that product are handled effectively and in accordance with the essential requirements set out in Section 2 of Annex I.

Commented [DN4]: This part has to be reworded. The lifetime is very different depending on the product category. Within machinery control systems are used for 10-20 years. Thus. it must be ensured that vulberabilities are handled by the manufacturer over the complete lifetime.

Also many consumer products are used over a significantly longer time period (slow moving consumer goods) such that consumers would have to incur security risks or replace products prematurely.

Unless the time period is extended significantly, the point of reference to determine the time period should not be the placing on the market, but the **making available**. Otherwise, especially low-income consumers would be severely disadvantaged: even though older generations of connected products are often more affordable and are still functional, they would not be secure to be used.

Manufacturers shall have appropriate policies and procedures, including coordinated vulnerability disclosure policies, referred to in Section 2, point (5), of Annex I, to process and remediate potential vulnerabilities in the product with digital elements reported from internal or external sources.

7. Before placing a product with digital elements on the market, manufacturers shall draw up the technical documentation referred to in Article 23.

They shall carry out the chosen conformity assessment procedures referred to in Article 24 ~~or have them carried out.~~

Where compliance of the product with digital elements with the essential requirements set out in Section 1 of Annex I and of the processes put in place by the manufacturer with the essential requirements set out in Section 2 of Annex I has been demonstrated by that conformity assessment procedure, manufacturers shall draw up the EU declaration of conformity in accordance with Article 20 and affix the CE marking in accordance with Article 22.

8. Manufacturers shall keep the technical documentation and the EU declaration of conformity, ~~where relevant,~~ at the disposal of the market surveillance authorities for ten years after the product with digital elements has been placed on the market.

9. Manufacturers shall ensure that procedures are in place for products with digital elements that are part of a series of production to remain in conformity with this regulation. The manufacturer shall adequately take into account changes in the development and production process or in the design or characteristics of the product with digital elements and changes in the harmonised standards, European cybersecurity certification schemes or the common specifications referred to in Article 19 by reference to which the conformity of the product with digital elements is declared shall be adequately taken into account ~~or by application of which its conformity is verified~~.

10. Manufacturers shall ensure that products with digital elements are accompanied by the information and instructions set out in Annex II, in an accessible electronic or physical form. Such information and instructions shall be in a language which can be easily understood by users. They shall be clear, understandable, intelligible and legible. They shall allow for a secure installation, operation and use of the products with digital elements.

11. Manufacturers shall either provide the EU declaration of conformity with the product with digital elements or include in the instructions and information set out in Annex II the internet address at which the EU declaration of conformity can be accessed. If the EU declaration of conformity is provided by digital means, it shall be accessed online for at least 10 years after placing on the market or putting into service of a product with digital elements.

12. From the placing on the market and for the expected product lifetime or for a period of five years after the placing on the market of a product with digital elements, whichever is shorter, manufacturers who know or have reason to believe that the product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential requirements set out in Annex I shall immediately take the corrective measures necessary to bring that product with digital elements or the manufacturer's processes into conformity, to withdraw or to recall the product, as appropriate.

Commented [DN5]: According to the NLF it maintains the only task of the manufacturer to carry out the conformity assessment.

Commented [DN6]: No added value.

Commented [DN7]: The higlighted part must be reworded according to Article R2 of Decision 768/2008/EC.

Commented [DN8]: NLF alignment accoring to Article R2 of Decision 768/2008/EC

Commented [DN9]: User shall be able to recognise that information and instructions before the purchase decision.

Commented [DN10]: Information and instructions shall be easy to find and as accessible as possible.
EN 301 549 and WCAG 2.2. shall be considered appropriatelly in regard to electronic documents and websites.

Commented [DN11]: Otherwise there is no indication of the minimum period of time within the DoC must be available.
The period of "10 years" are coming form the obligation for the manufacturer to keep the DoC at the disposal of the national authorities.

Commented [DN12]: Please see remarks to para 6.

13. Manufacturers shall, further to a reasoned request from a competent national ~~market surveillance~~ authority, provide that authority, in a language which can be easily understood by it, with all the information and documentation, in paper or electronic form, necessary to demonstrate the conformity of the product with digital elements and of the processes put in place by the manufacturer with the essential requirements set out in Annex I. They shall cooperate with that authority, at its request, on any measures taken to eliminate the cybersecurity risks posed by the product with digital elements, which they have placed on the market.

15. The Commission may, by means of implementing acts, specify the format and elements of the software bill of materials set out in Section 2, point (1), of Annex I. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2).

Article 11

Reporting obligations of manufacturers

1. The manufacturer shall, without undue delay and in any event within 24 hours of becoming aware of it, notify to ENISA any actively exploited vulnerability contained in the product with digital elements. The notification shall include details concerning that vulnerability and, where applicable, any corrective or mitigating measures taken. ENISA shall, without undue delay, unless for justified cybersecurity risk-related grounds, forward the notification to the CSIRT designated for the purposes of coordinated vulnerability disclosure in accordance with Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] of Member States concerned upon receipt and inform the market surveillance authorities of all concerned Member States~~y~~ about the notified vulnerability.

2. The manufacturer shall, without undue delay and in any event within 24 hours of becoming aware of it, notify to ENISA any incident having impact on the security of the product with digital elements. ENISA shall, without undue delay, unless for justified cybersecurity risk-related grounds, forward the notifications to the single point of contact designated in accordance with Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] of the Member States concerned and inform the market surveillance authority about the notified incidents. The incident notification shall include information on the severity and impact of the incident and, where applicable, indicate whether the manufacturer suspects the incident to be caused by unlawful or malicious acts or considers it to have a cross-border impact.

3. ENISA shall submit to the European cyber crisis liaison organisation network (EU-CyCLONe) established by Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] information notified pursuant to paragraphs 1 and 2 if such information is relevant for the coordinated management of large-scale cybersecurity incidents and crises at an operational level. ENISA should set up and operate a platform that empowers the Member States to perform Multi Stakeholder Vulnerability Disclosure Processes on a CSIRT level.

4. The manufacturer shall inform, without undue delay and after becoming aware, the users of the product with digital elements about the incident and, where necessary, about corrective measures that the user can deploy to mitigate the impact of the incident in a standardized, structured and easily automatically processable machine-readable format.

Commented [DN13]: NLF Alignment according to R2 of Decision 768/2008/EC

Commented [DN14]: We would prefer an electronic form for the national competent authority

Commented [DN15]: The specific format of the SBoM should not be described by an Implementing Act afterwards. However, it should at least be made clear that the SBoM must be drawn up directly, even if no specific format is specified.

Commented [DN16]: For the purpose of a better reading this should be the para 7.

Commented [DN17]: Not only with a look at this article, it is highly doubtful that ENISA will be able to provide the requested services without neglecting other tasks. Therefore, a discussion of the tasks of ENISA is needed.
Furthermore already existing reporting obligations should be assessed to avoid double reporting channels.
Therefore, it might be better to use already existing reporting channels by DORA and NIS regulation.

Commented [DN18]: 24 hours might be too short for a diligent analsysis of a vulnerability

Commented [DN19]: « The notification shall confirm with the machine readable format for security advisories, the Common Security Advisory Framework (CSAF) 2.0 and can addionally contain other formats »
Establish the basis for automation, based on commonly used machine readable standard

Commented [DN20]: What would be the « justified cybersecurity risk-related grounds » ?

Commented [DN21]: This will probably lead to double notifications with NIS2.

Commented [DN22]: The notification of « any incident » could overwhelm the authority. Maybe the term of « significant incident » according to NIS2 is better.

Commented [DN23]: Paragraphs subject to further review and clarification for dual-use products that are used in military or defence context. Clarification needed whether regulation needs to be adapted or further exeption rules have to be added. For intance, exeption rule could be added regarding 24-hour notification period to ENISA (Article 11 No. 1 and 2 CRA). It would also be conceivable to extend the notification period for all products in connection with a confidential notification of identified vulnerabilities until they have been remedied.

Commented [DN24]: This should not affect the obligation for information according to Article 34 of Regulation (EU) 2016/679.

5. The Commission may, by means of implementing acts, specify further the type of information, format and procedure of the notifications submitted pursuant to paragraphs 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2).

6.

Article 12

Authorised representatives

1. A manufacturer may, by a written mandate, appoint an authorised representative.
2. The obligations laid down in Article 10(1) to (7) first indent and (9) shall not form part of the authorised representative's mandate.

Article 13

Obligations of importers

1. Importers shall place only compliant products on the Community market. ~~Importers shall only place on the market products with digital elements that comply with the essential requirements set out in Section 1 of Annex I and where the processes put in place by the manufacturer are compliant with the essential requirements set out in Section 2 of Annex I.~~
2. Before placing a product with digital elements on the market, importers shall ensure that:
   (a) the appropriate conformity assessment procedures referred to in Article 24 have been carried out by the manufacturer;
   (b) the manufacturer has drawn up the technical documentation;
   (c) the product with digital elements bears the CE marking referred to in Article 22 and is accompanied by the information and instructions for use as set out in Annex II.
3. Where an importer considers or has reason to believe that a product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential requirements set out in Annex I, the importer shall not place the product on the market until that product or the processes put in place by the manufacturer have been brought into conformity with the essential requirements set out in Annex I. Furthermore, where the product with digital elements presents a significant cybersecurity risk, the importer shall inform the manufacturer and the market surveillance authorities to that effect.
4. Importers shall indicate their name, registered trade name or registered trademark, the postal address and if available, a digital contact ~~the email address~~ at which they can be contacted on the product with digital elements or, where that is not possible, on its packaging or in a document accompanying the product with digital elements. The contact details shall be in a language easily understood by users and market surveillance authorities.
6. Importers who know or have reason to believe that a product with digital elements, which they have placed on the market, or the processes put in place by its manufacturer, are not in conformity with the essential requirements set out in Annex I shall immediately take the corrective measures necessary to bring that product with digital elements or the processes put in place by its manufacturer into conformity with the essential requirements set out in Annex I, or to withdraw or recall the product, if appropriate.

Commented [DN25]: This should not be done afterwards. In order to give more security for the manufacturer this should be defined from the beginning on. For the possibility of amending those specifications such an implementing act could be helpful.

Commented [DN26]: This must be reworded according to R3 of Decision 768/2008/EC

Commented [DN27]: 1) This part has to be part of paragraph (1) according to R3 of Decision 768/2008/EC

2) According R3 of Decision 768/2008/EC only Art. 10 (1) and the drawing up of the technical documentation shall not form part of the authorised representative's mandate.

Thus this paragraph has to be reworded and moved to paragraph (1).

Commented [DN28]: Rewording accoirding to R4 of Decision 786/2008/EC

Commented [DN29]: This paragrahp has to be shifted to paragraph (2) according to R4 of Decision 768/2008/EC.

Commented [DN30]: Editorial alignment to the future Machinery Regulation.

Upon identifying a vulnerability in the product with digital elements, importers shall inform the manufacturer without undue delay about that vulnerability. Furthermore, where the product with digital elements presents a significant cybersecurity risk, importers shall immediately inform the competent national ~~market surveillance~~ authorities of the Member States in which they made the product with digital elements available on the market to that effect, giving details, in particular, of the non-conformity and of any corrective measures taken.

8. Importers shall, further to a reasoned request from a competent national ~~market surveillance~~ authority, provide it with all the information and documentation, in paper or electronic form, necessary to demonstrate the conformity of the product with digital elements with the essential requirements set out in Section 1 of Annex I as well as of the processes put in place by the manufacturer with the essential requirements set out in Section 2 of Annex I in a language that can be easily understood by that authority. They shall cooperate with that authority, at its request, on any action ~~measures~~ taken to eliminate the cybersecurity risks posed by a product with digital elements, which they have placed on the market.

9. When the importer of a product with digital elements becomes aware that the manufacturer of that product ceased its operations and, as result, is not able to comply with the obligations laid down in this Regulation, the importer shall inform the relevant competent national ~~market surveillance~~ authorities about this situation, as well as, by any means available and to the extent possible, the users of the products with digital elements placed on the market.

Article 14

Obligations of distributors

2. Before making a product with digital elements available on the market, distributors shall verify that:

(a) the product with digital elements bears the CE marking;

(b) the manufacturer and the importer have complied with the obligations set out respectively in Articles 10(10), 10(11) and 13(4).

3. Where a distributor considers or has reason to believe that a product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential requirements set out in Annex I, the distributor shall not make the product with digital elements available on the market until that product or the processes put in place by the manufacturer have been brought into conformity. Furthermore, where the product with digital elements poses a significant cybersecurity risk, the distributor shall inform without undue delay the manufacturer and the market surveillance authorities to that effect.

4. Distributors who know or have reason to believe that a product with digital elements, which they have made available on the market, or the processes put in place by its manufacturer are not in conformity with the essential requirements set out in Annex I shall make sure that the corrective measures necessary to bring that product with digital elements or the processes put in place by its manufacturer into conformity are taken, or to withdraw or recall the product, if appropriate.

Commented [DN31]: The correct term is "competent national authorities" according to R4 of Decision 768/2008/EC.

Commented [DN32]: The correct term is "competent national authorities" according to R4 of Decision 768/2008/EC.

Commented [DN33]: The correct word is "action" according to R4 of Decision 768/2008/EC.

Commented [DN34]: The correct term is "competent national authorities" according to R4 of Decision 768/2008/EC.

Commented [DN35]: In its current wording, any platform or website hosting open-source software (e.g. GitHub) would be included as a „distributor". This is surely unintentional and should be clarified.

Commented [DN36]: According to R5 of Decision 768/2008/EC this paragraph is part of paragraph (2).

Upon identifying a vulnerability in the product with digital elements, distributors shall inform the manufacturer without undue delay about that vulnerability. Furthermore, where the product with digital elements presents a significant cybersecurity risk, distributors shall immediately inform the national competent ~~market surveillance~~ authorities of the Member States in which they have made the product with digital elements available on the market to that effect, giving details, in particular, of the non-conformity and of any corrective measures taken.

5. Distributors shall, further to a reasoned request from a national competent ~~market surveillance~~ authority, provide it with all the information and documentation, in paper or electronic form, necessary to demonstrate the conformity of the product with digital elements and the processes put in place by its manufacturer with the essential requirements set out in Annex I in a language that can be easily understood by that authority. They shall cooperate with that authority, at its request, on any measures taken to eliminate the cybersecurity risks posed by a product with digital elements, which they have made available on the market.

6. When the distributor of a product with digital elements becomes aware that the manufacturer of that product ceased its operations and, as result, is not able to comply with the obligations laid down in this Regulation, the distributor shall inform without undue delay the relevant market surveillance authorities about this situation, as well as, by any means available and to the extent possible, the users of the products with digital elements placed on the market.

Article 16

Other cases in which obligations of manufacturers apply

A natural or legal person, ~~other than the manufacturer, the importer or the distributor,~~ that carries out a substantial modification of the product with digital elements shall be considered a manufacturer for the purposes of this Regulation.

That person shall be subject to the obligations of the manufacturer set out in Articles 10 and 11(1), (2), (4) and (7)~~, for the part of the product that is affected by the substantial modification or, if the substantial modification has an impact on the cybersecurity of the product with digital elements as a whole, for the entire product~~.

Commented [DN37]: In what respect

Commented [DN38]: This part must be deleted, because every person who carries out a substantial modificiation becomes a manufacturer.

Commented [DN39]: The highlighted part must be reworded.

If someone carries out a substantial modificatio that person becomes the manufacturer of the WHOLE product and not only of a specific part.

ANNEX I

ESSENTIAL CYBERSECURITY REQUIREMENTS

1. Security requirements relating to the properties of products with digital elements

(1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks;

(1) Products with digital elements shall be delivered without any known exploitable or built-in vulnerabilities;

(2) On the basis of the risk assessment referred to in Article 10(2) and where applicable, products with digital elements shall:

(a) be delivered with a secure by default configuration, including the possibility to reset the product to its original state;

(b) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems;

(c) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms;

(d) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, as well as report on corruptions;

(e) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended use of the product ('minimisation of data');

(f) protect the availability of essential functions, including the resilience against and mitigation of denial of service attacks;

(g) minimise ~~their own~~the negative impact by themselves or connected devices on the availability of services provided by other devices or networks;

(h) be designed, developed and produced to limit attack surfaces, including external interfaces;

(i) be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;

(j) provide security related information by recording and/or monitoring relevant internal activity, including the access to or modification of data, services or functions;

(k) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic updates and the notification of available updates to users.

(l) have a unique product identifier which allows the digital identification of the products . This unique product identifier is referenced in the security updates allowing an easy determination of the applicability of the patch.

Commented [DN40]: Known to whom ? responsibilities should be clear.

Commented [DN41]: What is an exploitable vulnerability?
Which vulnerability is not exploitable?
Should be more specific…

Commented [DN42]: Proposal to complement "usable security" as seperate subparagraph, since security related settings shall be designed with respect to human performance, enabling users to take measures intuitively. This is to enhance the specific objectice (iv) as declared in No 1 "CONTEXT OF THE PROPOSAL".

Commented [DN43]: Proposal to be more prezise.

Commented [DN44]: Addition because:
Identifying if a patch is applicable to a product is surprisingly challenging for industrial products due to the long livetime and changes in hardware and firmware. Sometimes a patch is only necessary for a specific combination of hard- and firmware. And the name of a prodict might change during its lifetime. For example if a company is acquired by another company often the names of the products change or during the lifetime of an industrial product the name is changed due to marketing purposes.

~~(k)~~(m) provide the possibility for users to securely and easily remove all data and settings (including those enabling access to specific networks) from the products and transfer the data safely to other products or systems to allow for a secure disposal of the product.

2. Vulnerability handling requirements

(4) once a security update has been made available, publically disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity clear and user friendly and information helping users to remediate the vulnerabilities where applicable and appropriate in a standardized, structured and easily automatically processable machine-readable format;

(7) provide for mechanisms to securely distribute updates for products with digital elements to ensure that ~~exploitable~~ vulnerabilities are fixed or mitigated in a timely manner;

ANNEX II

INFORMATION AND INSTRUCTIONS TO THE USER

As a minimum, the product with digital elements shall be accompanied by:

6. ~~if and, where applicable, where the software bill of materials can be accessed;~~

8. the type of technical security support offered by the manufacturer and until which date the manufacturer will provide it at the very least, as a bare minimum however, the expected product lifetime or until which date users can expect to receive security updates at the very least.~~when it will be provided, at the very least until when users can expect to receive security updates;~~ This information shall be distinctive and accessible before the purchase decision.

9. detailed and clear instructions and information in an user friendly language or an internet address referring to such detailed instructions and information on:

Commented [DN45]: The requirements so far only address the design and use phase, not the end of a product lifecycle. A secure and easy way to remove all data is an important prerequisite to promote a consumer-friendly way of recycling connected products.

Commented [DN46]: The CSAF Standard is ready to use and there is no reason not to give manufactures the time to prepare to implement it. https://csaf.io

Commented [DN47]: Referring to the targets of this proposal, security information for consumer IoT should already be available before making a buying decision. They should be barrier-free accessible, visible and easy to understand.

Commented [DN48]: This accompanying "information leaflet" is an one-off piece distributed with the product. It does not take into account the life-span of a product (which may be up to 10 years or more). We recommend more consumer oriented, user-centric dynamic information, as technical details or requirements may easily change during a products lifecycle. Information should be avaialbe to users until the end of the lifecycle of the product for example by affixing additional elements as URL link or QR code.

Commented [DN49]: Manufacturers should not be forced to make the software bill of materials publicly available.

FRANCE

Considérants

(6) To increase the overall level of cybersecurity of all products with digital elements placed on the internal market, it is necessary to introduce objective-oriented and technology-neutral essential cybersecurity requirements for these products that apply horizontally

(…)

(19) ~~Certain tasks provided for in this Regulation should be carried out by ENISA, in accordance with Article 3(2) of Regulation (EU) 2019/881. In particular, ENISA should receive notifications from manufacturers of actively exploited vulnerabilities contained in products with digital elements, as well as incidents having an impact on the security of those products. ENISA should also forward these notifications to the relevant Computer Security Incident Response Teams (CSIRTs) or, respectively, to the relevant single points of contact of the Member States designated in accordance with Article [Article X] of Directive [Directive XXX / XXXX (NIS2)], and inform the relevant market surveillance authorities about the notified vulnerability~~. The designated CSIRT from directive 2022/2555 should act as a coordinator, acting as a trusted intermediary with the manufacturers or providers, which are likely to be affected by the vulnerability. With the publicly available informations, ~~On the basis of the information it gathers,~~ ENISA should prepare a biennial technical report on emerging trends regarding cybersecurity risks in products with digital elements and submit it to the Cooperation Group referred to in Directive [Directive XXX / XXXX (NIS2)]. ~~Furthermore, considering its expertise and mandate, ENISA should be able to support the process for implementation of this Regulation.~~ In particular, it should be able to propose joint activities to be conducted by market surveillance authorities based on indications or information regarding potential non-compliance with this Regulation of products with digital elements across several Member States or identify categories of products for which simultaneous coordinated control actions should be organised. ~~In exceptional circumstances, at the request of the Commission, ENISA should be able to conduct evaluations in respect of specific products with digital elements that present a significant cybersecurity risk, where an immediate intervention is required to preserve the good functioning of the internal market.~~

(20) Products with digital elements should bear the CE marking to indicate their conformity with this Regulation so that they can move freely within the internal market. Member States should not create unjustified obstacles to the placing on the market of products with digital elements that comply with the requirements laid down in this Regulation and bear the CE marking.

(…)

Commented [CM50]: French authorities consider this recital to be in breach of the provisions and philosophy of Directive 2022/2555 (eg. Recitals 61 and 62, article 11, article 12), where CSIRTs are the first recipients of vulnerabilities.
In addition, certain elements present in the directive 2022/2555 establish a legal protection framework to report vulnerabilities and allow competent authorities, in coordination with the manufacturer, to identify patchs before vulnerabilities become publicly known.

National competent authority can maintain a deep level of trust and a good knowledge of the ecosystem thanks to the various coordination processes, the addition of an intermediary can undermine this trust and lead to the lost valuable information. Placing ENISA as an intermediary could lengthen process and thus unnecessarily increasing the window of exposure to exploit of a vulnerability. This would not be in line with international best practice guidelines on the topic, including OECD recommendations.

Hence, French authorities would like to preserve the philosophy where CSIRT of a MS remains the first recipient of this notification before informing ENISA.

Commented [CM51]: In line with the previous comment. We do not consider that CSA gives this mandate to ENISA.

Commented [CM52]: French authorities do not consider ENISA should carry out such activities. We still consider that this task is not cover by the mandate given by CSA. More, ENISA do not have the competences of a market surveillance authority.

(22) In order to ensure that products with digital elements, when placed on the market, do not pose cybersecurity risks to persons and organisations, essential requirements should be set out for such products. When the products are subsequently modified, by physical or digital means, in a way that is not foreseen by the manufacturer and that may imply that they no longer meet the relevant essential requirements, the modification should be considered as substantial. For example, software updates or repairs could be assimilated to maintenance operations provided that they do not modify a product already placed on the market in such a way that compliance with the applicable requirements may be affected, or that the intended use for which the product has been assessed may be changed. As is the case for physical repairs or modifications, a product with digital elements should be considered as substantially modified by a software change where the software update modifies the original intended functions, type or performance of the product and these changes were not foreseen in the initial risk assessment, or the nature of the hazard has changed or the level of risk has increased because of the software update.

(23) In line with the commonly established notion of substantial modification for products regulated by Union harmonisation legislation, whenever a substantial modification occurs that may affect the compliance of a product with this Regulation or when the intended purpose of that product changes, it is appropriate that the compliance of the product with digital elements is verified and that, where applicable, it undergoes a new conformity assessment. Where applicable, if the manufacturer undertakes a conformity assessment involving a third party, changes that might lead to substantial modifications should be notified to the third party.

(24) Refurbishing, maintaining and repairing of a product with digital elements, as defined in the Regulation [Eco-design Regulation], does not necessarily lead to a substantial modification of the product, for instance if the intended use and functionalities are not changed and the level of risk remains unaffected. However, upgrading a product by the manufacturer might lead to changes in the design and development of the product and therefore might affect the intended use and the compliance of the product with the requirements set out in this Regulation.

(…)

(32) In order to ensure that products with digital elements are secure both at the time of their placing on the market as well as throughout their life-cycle, it is necessary to lay down essential requirements for vulnerability handling and essential cybersecurity requirements relating to the properties of products with digital elements. While manufacturers should comply with all essential requirements related to vulnerability handling and ensure that all their products are delivered without any known exploitable vulnerabilities, they should determine which other essential requirements related to the product properties are relevant for the concerned type of product. For this purpose, manufacturers should undertake an assessment of the cybersecurity risks associated with a product with digital elements to identify relevant risks and relevant essential requirements and in order to appropriately apply suitable harmonised standards or common specifications.

Commented [CM53]: What is the definition of this life-cycle? Is there a regulatory definition of this notion of equipment life-cycle?
Also, is there a difference between product life-cycle and product lifetime (terms in art. 10 §6 for instance).

(33) In order to improve the security of products with digital elements placed on the internal market it is necessary to lay down essential requirements. These essential requirements should be without prejudice to the EU coordinated risk assessments of critical supply chains established by [Article X] of Directive [Directive XXX/XXXX(NIS2)][1], which take into account both technical and, where relevant, non-technical risk factors, such as undue influence by a third country on suppliers. Furthermore, it should be without prejudice to the Member States' prerogatives to lay down additional requirements that take account of non-technical factors for the purpose of ensuring a high level of resilience, including those defined in Recommendation (EU) 2019/534, in the Union-wide coordinated risk assessment of 5G networks security and in the EU Toolbox on 5G cybersecurity agreed by the NIS Cooperation Group as referred to in [Directive XXX/XXXX (NIS2)].

(34) To ensure that the national CSIRTs and the single point of contacts designated in accordance with Article [Article X] of Directive [Directive XX/XXXX (NIS2)] are provided with the information necessary to fulfil their tasks and raise the overall level of cybersecurity of essential and important entities, and to ensure the effective functioning of market surveillance authorities, manufacturers of products with digital elements should notify to ENISA vulnerabilities that are being actively exploited. As most products with digital elements are marketed across the entire internal market, any exploited vulnerability in a product with digital elements should be considered a threat to the functioning of the internal market. Manufacturers should also consider disclosing fixed vulnerabilities to the European vulnerability database established under Directive [Directive XX/XXXX (NIS2)] and managed by ENISA or under any other publicly accessible vulnerability database.

(35) Manufacturers should also report to ENISA any incident having an impact on the security of the product with digital elements. Notwithstanding the incident reporting obligations in Directive [Directive XXX/XXXX (NIS2)] for essential and important entities, it is crucial for ENISA, the single points of contact designated by the Member States in accordance with Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] and the market surveillance authorities to receive information from the manufacturers of products with digital elements allowing them to assess the security of these products. In order to ensure that users can react quickly to incidents having an impact on the security of their products with digital elements, manufacturers should also inform their users about any such incident and, where applicable, about any corrective measures that the users can deploy to mitigate the impact of the incident, for example by publishing relevant information on their websites or, where the manufacturer is able to contact the users and where justified by the risks, by reaching out to the users directly.

(36) Manufacturers of products with digital elements should put in place coordinated vulnerability disclosure policies to facilitate the reporting of vulnerabilities by individuals or entities. A coordinated vulnerability disclosure policy should specify a structured process through which vulnerabilities are reported to a manufacturer in a manner allowing the manufacturer to diagnose and remedy such vulnerabilities before detailed vulnerability information is disclosed to third parties or to the public. Given the fact that information about exploitable vulnerabilities in widely used products with digital elements can be sold at high prices on the black market, manufacturers of such products should be able to use programmes, as part of their coordinated vulnerability disclosure policies, to incentivise the reporting of vulnerabilities by ensuring that individuals or entities receive recognition and compensation for their efforts (so-called 'bug bounty programmes').

[1] Directive XXX of the European Parliament and of the Council of [date] [on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (OJ L xx, date, p.x)].

(37) In order to facilitate vulnerability analysis, manufacturers should identify and document components contained in the products with digital elements, including by drawing up a software bill of materials. A software bill of materials can provide those who manufacture, purchase, and operate software with information that enhances their understanding of the supply chain, which has multiple benefits, most notably it helps manufacturers and users to track known newly emerged vulnerabilities and risks. It is of particular importance for manufacturers to ensure that their products do not contain vulnerable components developed by third parties.

Commented [CM54]: French authorities would like to clarify the following point: is the software bill of materials intended to be
- an internal document meant for future conformity controls
- or aimed at being shared? final users, ENISA etc..

(…)

(42) Manufacturers should draw up an EU declaration of conformity to provide information required under this Regulation on the conformity of products with digital elements with the essential requirements of this Regulation and, where applicable, of the other relevant Union harmonisation legislation by which the product is covered. Manufacturers may also be required to draw up an EU declaration of conformity by other Union legislation. To ensure effective access to information for market surveillance purposes, a single EU declaration of conformity should be drawn up in respect of compliance with all relevant Union acts. In order to reduce the administrative burden on economic operators, it should be possible for that single EU declaration of conformity to be a dossier made up of relevant individual declarations of conformity.

(…)

Article 5

Requirements for products with digital elements

Products with digital elements shall only be made available on the market where:

(1) they meet the essential requirements set out in Section 1 of Annex I, under the condition that they are properly installed, maintained, used for their intended purpose or under conditions which can reasonably be foreseen, and, where applicable, updated, and

(2) the processes put in place by the manufacturer comply with the essential requirements set out in Section 2 of Annex I.

(…)

CHAPTER II

OBLIGATIONS OF ECONOMIC OPERATORS

Article 10

Obligations of manufacturers

1. When placing a product with digital elements on the market, manufacturers shall ensure that it has been designed, developed and produced in accordance with the essential requirements set out in Section 1 of Annex I.

2. For the purposes of complying with the obligation laid down in paragraph 1, manufacturers shall undertake an assessment of the cybersecurity risks associated with a product with digital elements and take the outcome of that assessment into account during the planning, design, development, production, delivery and maintenance phases of the product with digital elements with a view to minimising cybersecurity risks, preventing security incidents and minimising the impacts of such incidents, including in relation to the health and safety of users.

3. When placing a product with digital elements on the market, the manufacturer shall include a cybersecurity risk assessment in the technical documentation as set out in Article 23 and Annex V. For products with digital elements referred to in Articles 8 and 24(4) that are also subject to other Union acts, the cybersecurity risk assessment may be part of the risk assessment required by those respective Union acts. Where certain essential requirements are not applicable to the marketed product with digital elements, the manufacturer shall include a clear justification in that documentation.

4. For the purposes of complying with the obligation laid down in paragraph 1, manufacturers shall exercise due diligence when integrating components sourced from third parties in products with digital elements. They shall ensure that such components do not compromise the security of the product with digital elements.

Commented [CM55]: French authorities have questions on how this obligation will play for free software publishers and especially for equipment whose hardware manufacturer only provides the hardware system?

5. The manufacturer shall systematically document, in a manner that is proportionate to the nature and the cybersecurity risks, relevant cybersecurity aspects concerning the product with digital elements, including vulnerabilities they become aware of and any relevant information provided by third parties, and, where applicable, update the risk assessment of the product.

6. When placing a product with digital elements on the market, and for the expected product lifetime or for a period of five years from the placing of the product on the market, whichever is shorter, manufacturers shall ensure that vulnerabilities of that product are handled effectively and in accordance with the essential requirements set out in Section 2 of Annex I.

   Manufacturers shall have appropriate policies and procedures, including coordinated vulnerability disclosure policies, referred to in Section 2, point (5), of Annex I, to process and remediate potential vulnerabilities in the product with digital elements reported from internal or external sources.

Commented [CM56]: French authorities have questions regarding the application of the notion of "product lifetime" applied to this obligation.
A definition of "product lifetime" should be added to clarify the criteria to consider and what this term entails, how the lifetime of a product is estimated.

We support the comments made by the Netherlands on this paragraph and agree that "this concept lacks incentives for manufacturers to ensure that vulnerabilities are handled effectively for a reasonable period of time".
Users should be informed of the period of time during which vulnerabilities are handled effectively in any case.

7. Before placing a product with digital elements on the market, manufacturers shall draw up the technical documentation referred to in Article 23.

   They shall carry out the chosen conformity assessment procedures referred to in Article 24 or have them carried out.

   Where compliance of the product with digital elements with the essential requirements set out in Section 1 of Annex I and of the processes put in place by the manufacturer with the essential requirements set out in Section 2 of Annex I has been demonstrated by that conformity assessment procedure, manufacturers shall draw up the EU declaration of conformity in accordance with Article 20 and affix the CE marking in accordance with Article 22.

8. Manufacturers shall keep the technical documentation and the EU declaration of conformity, where relevant, at the disposal of the market surveillance authorities for ten years after the product with digital elements has been placed on the market.

9. Manufacturers shall ensure that procedures are in place for products with digital elements that are part of a series of production to remain in in compliance with the latest versions of standards related to CRA~~conformity~~. The manufacturer shall adequately take into account changes in the development and production process or in the design or characteristics of the product with digital elements and changes in the harmonised standards, European cybersecurity certification schemes or the common specifications referred to in Article 19 by reference to which the conformity of the product with digital elements is declared or by application of which its conformity is verified.

10. Manufacturers shall ensure that products with digital elements are accompanied by the information and instructions set out in Annex II, in an electronic or physical form. Such information and instructions shall be in a language which can be easily understood by users. They shall be clear, understandable, intelligible and legible. They shall allow for a secure installation, operation and use of the products with digital elements.

11. Manufacturers shall either provide the EU declaration of conformity with the product with digital elements or include in the instructions and information set out in Annex II the internet address at which the EU declaration of conformity can be accessed.

12. From the placing on the market and for the expected product lifetime or for a period of five years after the placing on the market of a product with digital elements, whichever is shorter, manufacturers who know or have reason to believe that the product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential requirements set out in Annex I shall immediately take the corrective measures necessary to bring that product with digital elements or the manufacturer's processes into conformity, to withdraw or to recall the product, as appropriate.

13. Manufacturers shall, further to a reasoned request from a market surveillance authority, provide that authority, in a language which can be easily understood by it, with all the information and documentation, in paper or electronic form, necessary to demonstrate the conformity of the product with digital elements and of the processes put in place by the manufacturer with the essential requirements set out in Annex I. They shall cooperate with that authority, at its request, on any measures taken to eliminate the cybersecurity risks posed by the product with digital elements, which they have placed on the market.

14. A manufacturer that ceases its operations and, as a result, is not able to comply with the obligations laid down in this Regulation shall inform, before the cease of operation takes effect, the relevant market surveillance authorities about this situation, as well as, by any means available and to the extent possible, the users of the concerned products with digital elements placed on the market.

15. The Commission may, by means of implementing acts, specify the format and elements of the software bill of materials set out in Section 2, point (1), of Annex I. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2).

Commented [CM57]: There is an ambiguity about the application of the standard over time.

Commented [CM58]: This part should remain consistent with the existing provisions in certain sectoral legislation: the simplified DoC is already defined and should therefore be recalled here (see for exemple art. 10.9 of EU Directive 2014/53/EU).

Commented [CM59]: Following the discussion of the last HPCWI, French authorities are open to discuss a balanced and realistic timeframe of the product life circle, for which manufacturers would have the obligation to cover risks.

Article 11

Reporting obligations of manufacturers

1. The manufacturer shall, without undue delay and in any event within 24 hours of becoming aware of it, notify to the CSIRT designated for the purposes of coordinated vulnerability disclosure in accordance with Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] of Member States concerned ~~to ENISA~~ any actively exploited vulnerability contained in the product with digital elements. The notification shall include technical details concerning that vulnerability ~~and, where applicable, any~~ corrective and/or mitigating measures and/or ~~taken, or~~ temporary workarounds identified, and when possible, measures to detect attempt to exploit the~~while a patch is being developped~~; ~~ENISA~~ The designated CSIRT shall, ~~without undue delay~~, unless for ~~justified~~ cybersecurity risk-related grounds, forward the notification to ~~the CSIRT designated for the purposes of coordinated vulnerability disclosure in accordance with Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] of Member States concerned~~ ENISA upon receipt and inform the market surveillance authority about the notified vulnerability.

2. The manufacturer shall, without undue delay and in any event within 24 hours of becoming aware of it, notify the single point of contact designated in accordance with Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] of the Member States concerned ~~to the designated CSIRT from the Directive 2022/2555 to ENISA~~ any incident having impact on the security of the product with digital elements. ~~ENISA~~ The designated CSIRT shall, ~~without undue delay~~, unless for ~~justified~~ cybersecurity risk-related grounds, forward the notifications to ~~the single point of contact designated in accordance with Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] of the Member States concerned~~ENISA and inform the market surveillance authority about the notified incidents. The incident notification shall include information on the severity and impact of the incident and, where applicable, indicate whether the manufacturer suspects the incident to be caused by unlawful or malicious acts or considers it to have a cross-border impact.

3. ENISA shall submit to the European cyber crisis liaison organisation network (EU-CyCLONe) established by Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] information notified pursuant to paragraphs 1 and 2 if such information is relevant for the coordinated management of large-scale cybersecurity incidents and crises at an operational level.

4. The manufacturer shall inform, without undue delay and after becoming aware, the users of the product with digital elements about the incident and, where necessary, about corrective measures that the user can deploy to mitigate the impact of the incident.

5. The Commission may, by means of implementing acts, specify further the type of information, format and procedure of the notifications submitted pursuant to paragraphs 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2).

6. ENISA, on the basis of the notifications received pursuant to paragraphs 1 and 2, shall prepare a biennial technical report on emerging trends regarding cybersecurity risks in products with digital elements and submit it to the Cooperation Group referred to in Article [Article X] of Directive [Directive XXX/XXXX (NIS2)]. The first such report shall be submitted within 24 months after the obligations laid down in paragraphs 1 and 2 start applying.

Commented [CM60]: As expressed by many MS during the last HPCW, French authorities do not support a notification system where the manufacturer shall directly report to ENISA.

Indeed, French authorities underline the following concerns

1) This new process questions the role of national authorities regarding vulnerabilities notification process
2) Coordination with the process established by NIS 2 (risk of ambiguity / confusion for economic operators)
3) Capacity to deal with the amount of notifications.

Has the Commission or the Presidency considered NCCA to be the point of contact?

Commented [CM61]: This addition to cover the situation where a patch takes time to develop (sometimes it can take months, because the vulnerability is complex to fix). In the absence of a patch, it is better to have a workaround.

In addition, software publishers sometimes have no choice but to publish the vulnerability (because a researcher is threatening to publish it or it is too critical not to publish it) and if the patch has not yet been developed, workarounds must be shared.

Commented [CM62]: French authorities would like to suggest to create a mirrored paragraph for manufacturer to inform weh possible, users after becoming aware of any actively exploited vulnerability

7. Manufacturers shall, upon identifying a vulnerability inform and co-ordinate remediation efforts with upstream and downstream stakeholders when the code vulnerability is embedded in third-party products (e.g. multi-party or supply chain co-ordination). ~~in a component, including in an open source component, which is integrated in the product with digital elements, report the vulnerability to the person or entity maintaining the component.~~

Commented [CM63]: Proposition of modification based on the OECD Good Practice Guidance on the Co-ordination of Digital Security Vulnerabilities OECD Legal Instruments

Article 12

Authorised representatives

1. A manufacturer may appoint an authorised representative by a written mandate.
2. The obligations laid down in Article 10(1) to (7) first indent and (9) shall not form part of the authorised representative's mandate.
3. An authorised representative shall perform the tasks specified in the mandate received from the manufacturer. The mandate shall allow the authorised representative to do at least the following:
   (a) keep the EU declaration of conformity referred to in Article 20 and the technical documentation referred to in Article 23 at the disposal of the market surveillance authorities for ten years after the product with digital elements has been placed on the market;
   (b) further to a reasoned request from a market surveillance authority, provide that authority with all the information and documentation necessary to demonstrate the conformity of the product with digital elements;
   (c) cooperate with the market surveillance authorities, at their request, on any action taken to eliminate the risks posed by a product with digital elements covered by the authorised representative's mandate.

Article 13

Obligations of importers

1. Importers shall only place on the market products with digital elements that comply with the essential requirements set out in Section 1 of Annex I and where the processes put in place by the manufacturer are compliant with the essential requirements set out in Section 2 of Annex I.
2. Before placing a product with digital elements on the market, importers shall ensure that:
   (a) the appropriate conformity assessment procedures referred to in Article 24 have been carried out by the manufacturer;
   (b) the manufacturer has drawn up the technical documentation;
   (c) the product with digital elements bears the CE marking referred to in Article 22 and is accompanied by the information and instructions for use as set out in Annex II.

3. Where an importer considers or has reason to believe that a product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential requirements set out in Annex I, the importer shall not place the product on the market until that product or the processes put in place by the manufacturer have been brought into conformity with the essential requirements set out in Annex I. Furthermore, where the product with digital elements presents a significant cybersecurity risk, the importer shall inform the manufacturer and the market surveillance authorities to that effect.

4. Importers shall indicate their name, registered trade name or registered trademark, the postal address and the email address at which they can be contacted on the product with digital elements or, where that is not possible, on its packaging or in a document accompanying the product with digital elements. The contact details shall be in a language easily understood by users and market surveillance authorities.

5. Importers shall ensure that the product with digital elements is accompanied by the instructions and information set out in Annex II in a language which can be easily understood by users.

6. Importers who know or have reason to believe that a product with digital elements, which they have placed on the market, or the processes put in place by its manufacturer, are not in conformity with the essential requirements set out in Annex I shall immediately take the corrective measures necessary to bring that product with digital elements or the processes put in place by its manufacturer into conformity with the essential requirements set out in Annex I, or to withdraw or recall the product, if appropriate.

   Upon identifying a vulnerability in the product with digital elements, importers shall inform the manufacturer without undue delay about that vulnerability. Furthermore, where the product with digital elements presents a significant cybersecurity risk, 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, giving details, in particular, of the non-conformity and of any corrective measures taken.

7. Importers shall, for ten years after the product with digital elements has been placed on the market, keep a copy of the EU declaration of conformity at the disposal of the market surveillance authorities and ensure that the technical documentation can be made available to those authorities, upon request.

8. Importers shall, further to a reasoned request from a market surveillance authority, provide it with all the information and documentation, in paper or electronic form, necessary to demonstrate the conformity of the product with digital elements with the essential requirements set out in Section 1 of Annex I as well as of the processes put in place by the manufacturer with the essential requirements set out in Section 2 of Annex I in a language that can be easily understood by that authority. They shall cooperate with that authority, at its request, on any measures taken to eliminate the cybersecurity risks posed by a product with digital elements, which they have placed on the market.

9. When the importer of a product with digital elements becomes aware that the manufacturer of that product ceased its operations and, as result, is not able to comply with the obligations laid down in this Regulation, the importer shall inform the relevant market surveillance authorities about this situation, as well as, by any means available and to the extent possible, the users of the products with digital elements placed on the market.

Commented [CM64]: French authorities would like to uncover if the definition of "significant cybersecurity risk" can include vulnerabilities?

Commented [CM65]: French authorities are wondering if there is a difference between this process of information and the notification process?

Article 14

Obligations of distributors

1. When making a product with digital elements available on the market, distributors shall act with due care in relation to the requirements of this Regulation.

2. Before making a product with digital elements available on the market, distributors shall verify that:

   (a) the product with digital elements bears the CE marking;

   (b) the manufacturer and the importer have complied with the obligations set out respectively in Articles 10(10), 10(11) and 13(4).

3. Where a distributor considers or has reason to believe that a product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential requirements set out in Annex I, the distributor shall not make the product with digital elements available on the market until that product or the processes put in place by the manufacturer have been brought into conformity. Furthermore, where the product with digital elements poses a significant cybersecurity risk, the distributor shall inform the manufacturer and the market surveillance authorities to that effect.

4. Distributors who know or have reason to believe that a product with digital elements, which they have made available on the market, or the processes put in place by its manufacturer are not in conformity with the essential requirements set out in Annex I shall make sure that the corrective measures necessary to bring that product with digital elements or the processes put in place by its manufacturer into conformity are taken, or to withdraw or recall the product, if appropriate.

   Upon identifying a vulnerability in the product with digital elements, distributors shall inform the manufacturer without undue delay about that vulnerability. Furthermore, where the product with digital elements presents a significant cybersecurity risk, distributors shall immediately inform the market surveillance authorities of the Member States in which they have made the product with digital elements available on the market to that effect, giving details, in particular, of the non-conformity and of any corrective measures taken.

5. Distributors shall, further to a reasoned request from a market surveillance authority, provide it with all the information and documentation, in paper or electronic form, necessary to demonstrate the conformity of the product with digital elements and the processes put in place by its manufacturer with the essential requirements set out in Annex I in a language that can be easily understood by that authority. They shall cooperate with that authority, at its request, on any measures taken to eliminate the cybersecurity risks posed by a product with digital elements, which they have made available on the market.

6. When the distributor of a product with digital elements becomes aware that the manufacturer of that product ceased its operations and, as result, is not able to comply with the obligations laid down in this Regulation, the distributor shall inform the relevant market surveillance authorities about this situation, as well as, by any means available and to the extent possible, the users of the products with digital elements placed on the market.

Article 15

Cases in which obligations of manufacturers apply to importers, ~~and~~ distributors and fulfilment center

An importer, ~~or~~a distributor, or a *and fulfilment center* shall be considered a manufacturer for the purposes of this Regulation and shall be subject to the obligations of the manufacturer set out in Articles 10 and 11(1), (2), (4) and (7) where that importer or distributor 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 already placed on the market.

Commented [CM66]: To stay consistent with Regulation 2019/1020. This modification would imply the addition in art. 3 of the definition of fulfilment center which can be found in regulation 2019/1020

Article 16

Other cases in which obligations of manufacturers apply

A natural or legal person, other than the manufacturer, the importer or the distributor, that carries out a substantial modification of the product with digital elements shall be considered a manufacturer for the purposes of this Regulation.

That person shall be subject to the obligations of the manufacturer set out in Articles 10 and 11(1), (2), (4) and (7), for the part of the product that is affected by the substantial modification or, if the substantial modification has an impact on the cybersecurity of the product with digital elements as a whole, for the entire product.

Article 17

Identification of economic operators

1. Economic operators shall, on request and where the information is available, provide to the market surveillance authorities the following information:

   (a) name and address of any economic operator who has supplied them with a product with digital elements;

   (b) name and address of any economic operator to whom they have supplied a product with digital elements;

2. Economic operators shall be able to present the information referred to in paragraph 1 for ten years after they have been supplied with the product with digital elements and for ten years after they have supplied the product with digital elements.

(…)

ANNEX I

ESSENTIAL CYBERSECURITY REQUIREMENTS

3. Security requirements relating to the properties of products with digital elements

(8) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks;

(9) Products with digital elements shall be delivered without any known ~~exploitable~~ vulnerabilities;

(10) On the basis of the risk assessment referred to in Article 10(2) and where applicable, products with digital elements shall:

(a) be delivered with a secure by default configuration, including the possibility to reset the product to its original state;

(b) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems;

(c) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms;

(d) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, as well as report on corruptions;

(e) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended use of the product ('minimisation of data');

(f) protect the availability of essential functions, including the resilience against and mitigation of denial of service attacks;

(g) minimise their own negative impact on the availability of services provided by other devices or networks;

(h) be designed, developed and produced to limit attack surfaces, including external interfaces;

(i) be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;

(j) be designed to limit fraudulent use of the product

~~9.1.1.1.1.1.~~

~~(i)~~(k) provide security related information by recording and/or monitoring relevant internal activity, including the access to or modification of data, services or functions;

~~(j)~~(l) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic updates and the notification of available updates to users.

Commented [CM67]: French authorities would like to raise the different use in the text of the expression "placing on the market" while here the expression "delivered" is used.
The expression should be changed if referring to the same time reference and if not, the word should be defined in the definition sections.
The purpose is to bring legal certainty to economic operators.

Commented [CM68]: The CSA refers to "verify that ICT products, ICT services and ICT processes do not contain **known vulnerabilities".**

As such, French authorities would like to make sure that two concepts are not mixed up
1) Notification of known exploitable vulnerability (art. 11)
2)Products have to be delivered without know vulnerabilities

If the expression "any known exploitable vulnerabilities" should remain, we would like some analysis as to why there should be a difference of expression used in the CRA compared to the CSA.

Commented [CM69]: This expression is used for the first time here, French authorities would like to recommend to add its definition in art. 3.

Commented [CM70]: -Recital (15) states that "he essential requirements laid down by this Regulation include all the elements of the essential requirements referred to in Article 3(3), points (d), (e) and (f) of Directive 2014/53/EU"
-Article 3(3), point (f) of Directive 2014/53/EU states "that radio equipment supports certain features ensuring protection from fraud". This requirement is not covered by another essential requirement of the annexe I point 1(3).
-
The limitation could be "if that product enables the holder or user to transfer money, monetary value or virtual currency as defined in Article 2, point (d), of Directive (EU) 2019/713

Formatted: Indent: Left: 3.5 cm, No bullets or numbering

Commented [CM71]: The French authorities are supporting the comments and propositions made by Belgium

4. Vulnerability handling requirements

Manufacturers of the products with digital elements shall:

(11) identify and document vulnerabilities and components contained in the product, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product;

(12) in relation to the risks posed to the products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates, or by providing temporary workarounds while a patch is being developped will need to be put in place.;

(13) apply effective and regular tests and reviews, based on best practices, of the security of the product with digital elements;

(14) once a security update has been made available, if not available workarounds publically disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and information helping users to remediate the vulnerabilities;

(15) put in place and enforce a policy on coordinated vulnerability disclosure;

~~(15)~~(16) if security updates or workarounds are not available, information about vulnerabilities should be shared to customers or users only when possible

~~(16)~~(17) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;

~~(17)~~(18) provide for mechanisms to securely distribute updates for products with digital elements to ensure that exploitable vulnerabilities are fixed or mitigated in a timely manner;

~~(18)~~(19) ensure that, where security patches or updates are available to address identified security issues, they are disseminated without delay and free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken. Security updates should be made available for a minimum duration of 10 years.

Commented [CM72]: This addition to cover the situation where a patch takes time to develop (sometimes it can take months, because the vulnerability is complex to fix). In the absence of a patch, it is better to have a workaround.
In addition, software publishers sometimes have no choice but to publish the vulnerability (because a researcher is threatening to publish it or it is too critical not to publish it) and if the patch has not yet been developed, workarounds must be shared .

Commented [CM73]: These notions should be specified.
Referring to best practices gives manufacturers an idea of how often tests and reviews should be performed.

Commented [CM74]: This modification is based on the same line of argument that the addition in §2.

Commented [CM75]: This modification covers the situation where there is no patch nor workarounds available. Users at least should be informed about the vulnerabilities.

In addition, the said information should not be publicly disclosed in this case but only to users as it represents a threat. Attackers could exploit the vulnerability, and with no existing patch this could be very dangerous.

Commented [CM76]: French authorities believe it would be necessary in terms of good practices to compel manufacturers to provide security updates for a mandatory period of time.

ANNEX II

INFORMATION AND INSTRUCTIONS TO THE USER

As a minimum, the product with digital elements shall be accompanied by:

1. the name, registered trade name or registered trade mark of the manufacturer, and the postal address and the email address at which the manufacturer can be contacted, on the product or, where that is not possible, on its packaging or in a document accompanying the product;
2. the point of contact where information about cybersecurity vulnerabilities of the product can be reported and received;
3. the correct identification of the type, batch, version or serial number or other element allowing the identification of the product and the corresponding instructions and user information;
4. the intended use, including the security environment provided by the manufacturer, as well as the product's essential functionalities and information about the security properties;
5. any known or foreseeable circumstance, related to the use of the product with digital elements in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to significant cybersecurity risks;
6. if and, where applicable, where the software bill of materials can be accessed;
7. where applicable, the internet address at which the EU declaration of conformity can be accessed;
8. the type of technical security support offered by the manufacturer and until when it will be provided, at the very least until when users can expect to receive security updates;
9. detailed instructions or an internet address referring to such detailed instructions and information on:
   (a) the necessary measures during initial commissioning and throughout the lifetime of the product to ensure its secure use;
   (b) how changes to the product can affect the security of data;
   (c) how security-relevant updates can be installed;

the secure decommissioning of the product, including information on how user data can be securely removed.

Commented [CM77]: Need to be consistent with the rules already established by the other applicable sectoral regulations (simplified DoC) in the continuity of our comment regarding art. 10 §11. The purpose would be to use the simplified declaration of conformity already provided for by the RED.

Formatted: Normal, Space After: 10 pt, Line spacing: Multiple 1.15 li

SPAIN

ES Comments on Presidency SE -Block 2 of the Proposal of a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020

("Cyber Resiliency Act")

20 January 2023

Text proposed by the Commission	SPAIN Comments
RECITALS	
(19) Certain tasks provided for in this Regulation should be carried out by ENISA, in accordance with Article 3(2) of Regulation (EU) 2019/881. In particular, ENISA should receive notifications from manufacturers of actively exploited vulnerabilities contained in products with digital elements, as well as incidents having an impact on the security of those products. ENISA should also forward these notifications to the relevant Computer Security Incident Response Teams (CSIRTs) or, respectively, to the relevant single points of contact of the Member States designated in accordance with Article [Article X] of Directive [Directive XXX / XXXX (NIS2)], and inform the relevant market surveillance authorities about the notified vulnerability. On the basis of the information it gathers, ENISA should prepare a biennial technical report on emerging trends regarding cybersecurity risks in products with digital elements and submit it to the Cooperation Group referred to in Directive [Directive XXX / XXXX (NIS2)]. Furthermore, considering its expertise and mandate, ENISA should be able to support the process for implementation of this Regulation. In particular, it should be able to propose joint activities to be	The recital should be changed in 3 points. Implementing these points could lead to a new recital or even to new articles, as needed: • It should state that ENISA "Should support the process for implementation of this Regulation for all Member states that request it", not just "ENISA should be able to support the process for implementation of this Regulation". • ENISA's role should also offer services such as a common EU Registry of entities, products and vulnerabilities. This registry, after the model of the NIS2 Directive (art. 27), would be accessible to all market surveillance authorities. The entities to be included in this registry should at least encompass software producers and Classes I and II. • Also, we suggest to directly regulate in the CRA the continuous involvement of ENISA, which should not be limited to exceptional circumstances at the request of the Commission. This

conducted by market surveillance authorities based on indications or information regarding potential non-compliance with this Regulation of products with digital elements across several Member States or identify categories of products for which simultaneous coordinated control actions should be organised. In exceptional circumstances, at the request of the Commission, ENISA should be able to conduct evaluations in respect of specific products with digital elements that present a significant cybersecurity risk, where an immediate intervention is required to preserve the good functioning of the internal market.	continuous involvement of ENISA should be ensured particularly for "complex products", such as Operating Systems. Some Member States will need support in the supervision of these products, and this initiative needs to be developed at Union Level, with common resources and the involvement of ENISA. The main sourtce of probloems with these "complex products" is not that they are very numerous, but that they are very complex to review and monitor by Member states.
(24) **Refurbishing, maintaining and repairing** of a product with digital elements, as defined in the Regulation [Eco-design Regulation], does not necessarily lead to a substantial modification of the product, for instance if the intended use and functionalities are not changed and the level of risk remains unaffected. However, upgrading a product by the manufacturer might lead to changes in the design and development of the product and therefore might affect the intended use and the compliance of the product with the requirements set out in this Regulation.	This Regulation [Eco-design Regulation] is not yet published. So this recital must be reviewed after its publication, to check if any changes are needed. Particularly, the need to include the 3 definitions in Chapter 3 of definitions.

Article 5	
Requirements for products with digital elements	
Products with digital elements shall only be **made available on the market** where:	
(1) they meet the essential requirements set out in Section 1 of Annex I, **under the condition that they are properly installed, maintained, used for their intended purpose or under conditions which can reasonably be foreseen, and, where applicable, updated,** and	The wording of this part needs to be clarified. It's difficult to clearly understand. For sample, it is not clear whether the "proper installation" condition affects goods " made available on the market".
(2) the processes put in place by the manufacturer comply with the essential requirements set out in Section 2 of Annex I.	
Article 10	
Obligations of manufacturers	
12. From the placing on the market and for the expected product lifetime or for a period of **five years** after the placing on the market of a product with digital elements, whichever is shorter, manufacturers **who know or have reason to believe** that the product with digital elements or the processes put in place by the manufacturer **are not in conformity with the essential requirements** set out in Annex I shall **immediately take the corrective measures** necessary to bring that product with digital elements or the manufacturer's processes into conformity, to withdraw or to recall the product, as appropriate.	Proposal: to add a new paragraph to this point, as in Directive RED to radio equipment: "Furthermore, where a product with digital elements presents a cybersecurity risk, manufacturers shall immediately inform the competent national authorities of the Member States in which they made the digital product available on the market to that effect, giving details, in particular, of the non-compliance, of any corrective measures taken and of the results thereof." This is in line with the FR proposal of a change in Annex I point 2.3 to include the obligation to the manufactures to provide **mitigation measures** while the vulnerability is corrected.

Article 11	
Reporting obligations of manufacturers	
1. The manufacturer shall, without undue delay and in any event within **24 hours** of becoming aware of it, notify to ENISA **any actively exploited vulnerability contained in the product** with digital elements. The notification shall include details concerning that vulnerability and, where applicable, any corrective or mitigating measures taken. ENISA shall, without undue delay, unless for justified cybersecurity risk-related grounds, forward the notification to the CSIRT designated for the purposes of coordinated vulnerability disclosure in accordance with Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] of Member States concerned upon receipt and inform the market surveillance authority about the notified vulnerability.	A deadline of only 24 hours from the point of becoming aware of a vulnerability could be too short for SME's. Particularly, if checking and verification of the any actively exploited vulnerability is needed.
2. The manufacturer shall, without undue delay and in any event within **24 hours** of becoming aware of it, notify to ENISA **any incident having impact on the security of the product** with digital elements. ENISA shall, without undue delay, unless for justified cybersecurity risk-related grounds, forward the notifications to the single point of contact designated in accordance with Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] of the Member States concerned and inform the market surveillance authority about the notified incidents. The incident notification shall include information on the severity and impact of the incident and, where applicable, indicate whether the manufacturer suspects the incident to be caused by unlawful or malicious acts or considers it to have a cross-border impact.	A deadline of only 24 hours from the point of becoming aware of a vulnerability could be too short for SME's. Particularly, if checking and verification of the any actively exploited vulnerability is needed before notifying ENISA.

7. Manufacturers shall, upon identifying a vulnerability in a component, including in an open source component, which is integrated in the product with digital elements, report the vulnerability to the person or entity maintaining the component.	We propose to add : "as well as report the vulnerability to ENISA to register it".
Article 12	
Authorised representatives	
Article 13	
Obligations of importers	
4. Importers shall indicate their name, registered trade name or registered trademark, the postal address and the **email address** at which they can be contacted on the product with digital elements or, where that is not possible, on its packaging or in a document accompanying the product with digital elements. The contact details shall be in a language easily understood by users and market surveillance authorities.	**email address –** should be a "formal one", company email if possible . For better tracking by MSAs.
5. Importers shall ensure that the product with digital elements is accompanied by the **instructions and information** set out in **Annex II** in a language which can be easily understood by users.	Add the following as per in RED Directive: "… in a language which can be easily understood by users, **as determined by the Member State concerned in National Regulation of RED or EMC Directives."** For coherence with other requirements of the same product.
Article 14	
Obligations of distributors	
Upon identifying a vulnerability in the product with digital elements, distributors shall inform the manufacturer without undue delay about that vulnerability.	We propose to add : "as well as report the vulnerability to ENISA to register it".

Article 15	
Cases in which obligations of manufacturers apply to importers and distributors	
Article 16	
Other cases in which obligations of manufacturers apply	
A natural or legal person, other than the manufacturer, the importer or the distributor, that carries out a substantial modification of the product with digital elements shall be considered a manufacturer for the purposes of this Regulation. That person shall be subject to the obligations of the manufacturer set out in Articles 10 and 11(1), (2), (4) and (7), for the part of the product that is affected by the substantial modification or, if the substantial modification has an impact on the cybersecurity of the product with digital elements as a whole, for the entire product.	This should follow what is in the "Revision of the Machinery Directive 2006/42/EC.Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on machinery products". Particularly, making the total responsibility the "default mode" and partial responsibility something that must be somehow proven. E.G.: "A natural or legal person that carries out a substantial modification of a machinery or related product shall be considered a manufacturer for the purposes of this Regulation That person shall be subject to the obligations of the manufacturer set out in Articles 10 and 11(1), (2), (4) and (7), for that machinery or related product or, if the substantial modification has only an impact on the cybersecurity of a part of an assembly of machinery, for the affected machinery of this assembly as demonstrated in the risk assessment."

Article 17	
Identification of economic operators	
ANNEXES	
ANNEX I	
ESSENTIAL CYBERSECURITY REQUIREMENTS	
1.Security requirements relating to the properties of products with digital elements	
(2) Products with digital elements shall be **delivered** without any known exploitable vulnerabilities;	Clarification is needed . Is a product "delivered" is when the product gets to the user? , when it is sent in the mail? What happens if a known exploitable vulnerability is discovered when a product is already in the "supply chain"?
(3) On **the basis of the risk assessment** referred to in Article 10(2) and where applicable, products with digital elements shall:	**Proposal**: "the basis of the cybersecurity risks assessment.."
2. Vulnerability handling requirements	
Manufacturers of the products with digital elements shall:	
(3) apply effective and regular tests and reviews of the security of the product with digital elements;	What is of frequency of regular tests and reviews? Monthly, yearly,….?
ANNEX II	
INFORMATION AND INSTRUCTIONS TO THE USER	
9. **detailed instructions or an internet address** referring to such detailed instructions and information on:	Internet address : need to be more specific. For sample a an internet URL address.

ITALY

Italian National Cybersecurity Agency Comments on the Cyber Resilience Act

DRAFT, 18 January 2023

These comments are without prejudice to further positions the Italian National Cybersecurity Agency or other national authorities may provide on this matter.

1 Scope

1.1 Exclusion clause

Concerning the exclusion clause (paragraph 5, article 2), our position is to rephrase the terms "developed exclusively for" into "intended for use of".

Moreover, concerning the latest Presidency compromise proporsal, our position is to reintroduce the previously added paragraphs 5b and 5c of article 2, while supporting the addition of paragraph 3b of article 4.

Finally, we support the introduction of an additional paragraph safeguarding domestic jurisdiction. A possible phrasing could be as follows "Member State may adopt or maintain provision with a view to achieving a higher level of cybersecurity of products with digital elements".

1.2 Exclusion of non-connectable products with digital elements

As mentioned in our previous comments (WK 17303/2022), our position is to remove the scope limitation to only "connectable" products. That is, applying the Regulation to all products with digital elements independently from their capability to exchange data at the time of their placing on the market.

Therefore, paragraph 1 of article 2 would read as follows: "This regulation applies to product with digital elements". It greatly simplifies the text, making it future proof and less exposed to loopholes. This would also entail the deletion of confusion definitions such as "logical connection", "physical connection" and "indirect connection" (paragraphs 11, 12 and 13 of article 3).

1.3 Exclusion of services and software as a service

While a national position has not been finalized yet, we are sceptical on the exclusion of services from the scope of the Regulation (paragraph 1, article 3), with particular emphasis on Sofware-as-a-Service (recital 9).

In this regards, we do not see major differences in between the mentioned services and the "remote data processing" and have some concerns in the application of CRA on products that leverage SaaS services (who is responsible for what?).

The changes in the recital 9 in the latest Presidency compromise proposal are proceeding in the right direction but may not be sufficient.

Therefore, we would welcome additional explanations by the Commission as well as continuing the discussion on this topic in HWPCI and are inclined to support the position of those Member States asking for the full inclusion of services and SaaS in the scope of the Regulation.

1.4 Unfinished software and testing

Paragraph 4, article 4, mandates that "Member States shall not prevent the making available of unfinished software which does not comply with this Regulation provided that the software is only made available for a limited period required for testing purposes and that a visible sign clearly indicates that it does not comply with this Regulation and will not be available on the market for purposes other than testing".

While we do see the overarching goal of preventing hindrances to research and development, we have three concerns with respect to this provision:

1. some of the essential requirements laid down in Annex I cannot be implemented properly in between the testing and the production phase of a product, in particular considering software;
2. there is a growing trend of early (beta-testing) software releases for extended periods of time;
3. manufacturers may leverage this exemption as a loophole to avoid the application of CRA requirements.

We would welcome a discussion to address these concerns.

1.5 Patching and placing on the market concept

While recitals (22, 23 and 24) mention the interplay in between the placing on the market concept and the updates or modification to a digital product, we would like to prevent:

1. manufacturer from downplaying patch impact to avoid additional conformity assessments;
2. unduly delays the publication of patches by introducing additional conformity assessments;
3. deadlock and delays when publishing security patches.

To this end, we propose to introduce a fast-track. That is, allowing the placing on the market of a patch prior to the finalization of the conformity assessment procedure. In this case, the manufacturer should be responsible to fix any issue that may be identified in the conformity assessment procedure within a specified time-frame.

This fast-track procedure should be applicable to security patches, that can therefore be distributed without delays.

Manufacturer may also opt to submit non security patches to this fast-track in order to speed-up the release.

Moreover, it would be useful to lay down, in an annex or in subsequent guidelines, some objective criteria to distinguish between patches implying substantial and non-substantial modification and procedures, to ensure clarity and mitigate litigiousness with respect to the definition provided in article 3, paragraph 31. These criteria and procedure may be such as:

a. a patch rewriting 5% of the code is always deemed a substantial modification;
b. frequently patched products must be submitted to the fast-track at least once each two years;
c. refactoring is not considered a substantial modification.

1.6 Applicability of CRA to old products with substantial patches

Following from the previous point, it is unclear whether a software product that is placed on the market prior to the entry into force of the CRA:

1. will never be subject to its requirements; or
2. will be subject to its requirements after the first update entailing a substantial modification.

We would support the second options and welcome a clarification on this point by the Commission.

1.7 Open source

Recital 10 clarifies that "In order not to hamper innovation or research, free and open-source software developed or supplied outside the course of a commercial activity should not be covered by this Regulation.". While we agree with the overarching principle, we have two concerns with this provision:

1. inability for open-source software to achieve the CE marking;
2. impact on the commercial services offered by companies that do not control most of the code-base of the open-source software.

Concerning the former, we propose to introduce the possibility for open-source software to undergo the conformity assessment to achieve the CE marking on a voluntary basis. This would also benefit:

- consumers that may therefore differentiate between open-source projects that are willing to undergo some scrutiny with respect to those that won't;
- open-source itself as its otherwise inability to achieve the CE marking may hamper its usage by consumer that may understandably associate the lack of CE marking as an indicator of untrustworthiness.

Concerning the latter, the current formulation (in combination with article 10, paragraph 4) may prevent the usage of open-source software in commercial product, as the companies that use open-source libraries or embed third-party open-source product would then be responsible to perform due diligence and ensure that the security of their product is not compromised by pieces of software they do not control and that are not subject to CRA requirements , which may not be technically feasible. This may in turn be a blow to innovation or research limiting the industrial usage of open-source.

We would welcome a discussion to address this issue.

1.8 Micro and small enterprises

We would welcome a discussion concerning the impact, and possible necessary mitigation, of the application of CRA on micro and small enterprises.

2 Interplay with other EU regulation

2.1 Cyber Security Act

The Regulation implies two interactions in between CRA and CSA:

1. highly critical products, identified by the Commission through delegated acts adopted by the procedure outlined in article 50, may be subject to CSA certification to demonstrate conformity with the CRA essential requirements (article 6, paragraph 5);
2. products certified under CSA are presumed in conformity with the CRA essential requirements (article 18, paragraph 3).

To ensure the soundness of the latter, it should first be verified that the CSA certification scheme does include the CRA essential requirements

2.2 Interplay with Maritime and other sectoral regulations.

We would like to point out possible issues in the application of CRA with respect to products covered by Directive 2014/90 on marine equipment. We would therefore request a joint analysis on this topic by DG Connect, DG Move and DG Mare.

Generally speaking, we would welcome a broader analysis from the Commission to assess the impact of CRA with respect to EU legislation that tackles the concepts of conformity assessment and certification.

3 Definition of Product with digital elements

We are in the process of analysing the definition framework concerning products with digital elements (paragraphs 1, 2, 5, 6, 7, 8, 9 and 16 of article 3), which appears to be complex with a high risk of inconsistencies.

4 Reporting obligation

Concerning the reporting obligation of manufacturer framework outline in article 11, paragraph 1, our position is that ENISA should not be the primary and first contact point for vulnerabilities and incident notification from manufacturer as it would introduce a different information flow form those already in place for incidents (NIS/NIS2) and that are being put in place for coordinated vulnerability disclosure (NIS2), most likely introducing ambiguity, duplication, and confusion. Therefore, our position is that vulnerabilities and incident notification must be notified directly to the CSIRT or national cybersecurity authority of the relevant Member State(s). This would also allow to promptly activate the already existing structures for cross-border cooperation at technical level (CSIRT Network) and operational level (CyCLONe) without introducing any additional mechanism, while also providing the opportunity for synergies in the implementation of the CVD policy that must be developed at national level under NIS2.
This is without prejudice to a possible subsequent notification of vulnerabilities from the Member State to ENISA, as provided by NIS2 in the context of CVD.

5 Essential Requirments

A full examination of the essential requirements is still underway.

5.1 Vulnerabilities management timeframe

Paragraph 6 of article 10 limits the responsibility of manufacturers to manage vulnerabilities for the product lifetime or five years from the placing into market, whichever is shorter. This timeframe appears to be way shorter that the effective lifetime (i.e., the expected period of usage after purchase) of both consumer and industrial ICT products. Moreover, manufacturers may therefore tend to downplay the nominal lifetime of a product to further limit their responsibility in this context.
Therefore, to mitigate this issue, we propose to:

- define a minimum timeframe and increase the maximum timeframe in which manufacturer must ensure vulnerability management;
- require manufacturer to inform customer of the nominal product lifetime and the remainder of the period of vulnerability management;
- empower market surveillance authority to publish statistics on manufacturer behaviour in this context.

5.2 Vulnerabilities management requirements

We would welcome a strengthening of the essential requirements related to vulnerability management outlined in paragraph 6 of article 10 and in point 2 of annex I. In particular, we propose to:

- define a maximum timeframe for manufacturer to put into place remediation actions (including patching);
- empower market surveillance authority to publish statistics on manufacturer behaviour in this context.
- require manufacturer to adopt a policy on coordinated vulnerability disclosure compliant with the relevant policies being developed at national level under NIS2.

LATVIA

Latvia comments on CRA

Block 2

(6) To increase the overall level of cybersecurity of all products with digital elements placed on the internal market, it is necessary to introduce objective-oriented and technology-neutral essential cybersecurity requirements for these products that apply horizontally.

(19) Certain tasks provided for in this Regulation should be carried out by ENISA, in accordance with Article 3(2) of Regulation (EU) 2019/881. In particular, ENISA should receive notifications from manufacturers of actively exploited vulnerabilities contained in products with digital elements, as well as incidents having an impact on the security of those products. ENISA should also forward these notifications respectively to the relevant Computer Security Incident Response Teams (CSIRTs) or~~, respectively~~, to the relevant single points of contact of the Member States designated in accordance with Article [Article X] of Directive [Directive XXX / XXXX (NIS2)], and inform the relevant market surveillance authorities about the notified vulnerability. On the basis of the information it gathers, ENISA should prepare a biennial technical report on emerging trends regarding cybersecurity risks in products with digital elements and submit it to the Cooperation Group referred to in Directive [Directive XXX / XXXX (NIS2)]. Furthermore, considering its expertise and mandate, ENISA should be able to support the process for implementation of this Regulation. In particular, it should be able to propose joint activities to be conducted by market surveillance authorities based on indications or information regarding potential non-compliance with this Regulation of products with digital elements across several Member States or identify categories of products for which simultaneous coordinated control actions should be organised. In exceptional circumstances, at the request of the Commission, ENISA should be able to conduct evaluations in respect of specific products with digital elements that present a significant cybersecurity risk, where an immediate intervention is required to preserve the good functioning of the internal market.

(20) Products with digital elements should bear the CE marking to indicate their conformity with this Regulation so that they can move freely within the internal market. Member States should not create unjustified obstacles to the placing on the market of products with digital elements that comply with the requirements laid down in this Regulation and bear the CE marking.

(22) In order to ensure that products with digital elements, when placed on the market, do not pose cybersecurity risks to persons and organisations, essential requirements should be set out for such products. When the products are subsequently modified, by physical or digital means, in a way that is not foreseen by the manufacturer and that may imply that they no longer meet the relevant essential requirements, the modification should be considered as substantial. For example, software updates or repairs could be assimilated to maintenance operations provided that they do not modify a product already placed on the market in such a way that compliance with the applicable requirements may be affected, or that the intended use for which the product has been assessed may be changed. As is the case for physical repairs or modifications, a product with digital elements should be considered as substantially modified by a software change where the software update modifies the original intended functions, type or performance of the product and these changes were not foreseen in the initial risk assessment, or the nature of the hazard has changed or the level of risk has increased because of the software update.

(23) In line with the commonly established notion of substantial modification for products regulated by Union harmonisation legislation, whenever a substantial modification occurs that may affect the compliance of a product with this Regulation or when the intended purpose of that product changes, it is appropriate that the compliance of the product with digital elements is verified and that, where applicable, it undergoes a new conformity assessment. Where applicable, if the manufacturer undertakes a conformity assessment involving a third party, changes that might lead to substantial modifications should be notified to the third party.

(24) Refurbishing, maintaining and repairing of a product with digital elements, as defined in the Regulation [Eco-design Regulation], does not necessarily lead to a substantial modification of the product, for instance if the intended use and functionalities are not changed and the level of risk remains unaffected. However, upgrading a product by the manufacturer might lead to changes in the design and development of the product and therefore might affect the intended use and the compliance of the product with the requirements set out in this Regulation.

(32) In order to ensure that products with digital elements are secure both at the time of their placing on the market as well as throughout their life-cycle, it is necessary to lay down essential requirements for vulnerability handling and essential cybersecurity requirements relating to the properties of products with digital elements. While manufacturers should comply with all essential requirements related to vulnerability handling and ensure that all their products are delivered without any known exploitable vulnerabilities, they should determine which other essential requirements related to the product properties are relevant for the concerned type of product. For this purpose, manufacturers should undertake an assessment of the cybersecurity risks associated with a product with digital elements to identify relevant risks and relevant essential requirements and in order to appropriately apply suitable harmonised standards or common specifications.

(33) In order to improve the security of products with digital elements placed on the internal market it is necessary to lay down essential requirements. These essential requirements should be without prejudice to the EU coordinated risk assessments of critical supply chains established by [Article X] of Directive [Directive XXX/XXXX(NIS2)][2], which take into account both technical and, where relevant, non-technical risk factors, such as undue influence by a third country on suppliers. Furthermore, it should be without prejudice to the Member States' prerogatives to lay down additional requirements that take account of non-technical factors for the purpose of ensuring a high level of resilience, including those defined in Recommendation (EU) 2019/534, in the Union-wide coordinated risk assessment of 5G networks security and in the EU Toolbox on 5G cybersecurity agreed by the NIS Cooperation Group as referred to in [Directive XXX/XXXX (NIS2)].

Commented [SŽ78]: LV: sentence duplicates 1st sentence of Recital 22. Our suggestion is to delete this sentence.

(34) To ensure that the national CSIRTs and the single point of contacts designated in accordance with Article [Article X] of Directive [Directive XX/XXXX (NIS2)] are provided with the information necessary to fulfil their tasks and raise the overall level of cybersecurity of essential and important entities, and to ensure the effective functioning of market surveillance authorities, manufacturers of products with digital elements should notify to ENISA vulnerabilities that are being actively exploited. As most products with digital elements are marketed across the entire internal market, any exploited vulnerability in a product with digital elements should be considered a threat to the functioning of the internal market. Manufacturers should also consider disclosing fixed vulnerabilities to the European vulnerability database established under Directive [Directive XX/XXXX (NIS2)] and managed by ENISA or under any other publicly accessible vulnerability database.

[2] Directive XXX of the European Parliament and of the Council of [date] [on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (OJ L xx, date, p.x)].

(35) Manufacturers should also report to ENISA any incident having an impact on the security of the product with digital elements. Notwithstanding the incident reporting obligations in Directive [Directive XXX/XXXX (NIS2)] for essential and important entities, it is crucial for ENISA, the single points of contact designated by the Member States in accordance with Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] and the market surveillance authorities to receive information from the manufacturers of products with digital elements allowing them to assess the security of these products. In order to ensure that users can react quickly to incidents having an impact on the security of their products with digital elements, manufacturers should also inform their users about any such incident and, where applicable, about any corrective measures that the users can deploy to mitigate the impact of the incident, for example by publishing relevant information on their websites or, where the manufacturer is able to contact the users and where justified by the risks, by reaching out to the users directly.

(36) Manufacturers of products with digital elements should put in place coordinated vulnerability disclosure policies to facilitate the reporting of vulnerabilities by individuals or entities. A coordinated vulnerability disclosure policy should specify a structured process through which vulnerabilities are reported to a manufacturer in a manner allowing the manufacturer to diagnose and remedy such vulnerabilities before detailed vulnerability information is disclosed to third parties or to the public. Given the fact that information about exploitable vulnerabilities in widely used products with digital elements can be sold at high prices on the black market, manufacturers of such products ~~should be able to~~may use programmes, as part of their coordinated vulnerability disclosure policies, to incentivise the reporting of vulnerabilities by ensuring that individuals or entities receive recognition and compensation for their efforts (so-called 'bug bounty programmes').

Commented [SŽ79]: LV: we should take into account that SMEs will be mostly impacted by CRA. Majority most probably won't use bug bounty programmes.

(37) In order to facilitate vulnerability analysis, manufacturers should identify and document components contained in the products with digital elements, including by drawing up a software bill of materials. A software bill of materials can provide those who manufacture, purchase, and operate software with information that enhances their understanding of the supply chain, which has multiple benefits, most notably it helps manufacturers and users to track known newly emerged vulnerabilities and risks. It is of particular importance for manufacturers to ensure that their products do not contain vulnerable components developed by third parties.

(42) Manufacturers should draw up an EU declaration of conformity to provide information required under this Regulation on the conformity of products with digital elements with the essential requirements of this Regulation and, where applicable, of the other relevant Union harmonisation legislation by which the product is covered. Manufacturers may also be required to draw up an EU declaration of conformity by other Union legislation. To ensure effective access to information for market surveillance purposes, a single EU declaration of conformity should be drawn up in respect of compliance with all relevant Union acts. In order to reduce the administrative burden on economic operators, it should be possible for that single EU declaration of conformity to be a dossier made up of relevant individual declarations of conformity.

Article 5

Requirements for products with digital elements

Products with digital elements shall only be made available on the market where:

(1) they meet the essential requirements set out in Section 1 of Annex I, under the condition that they are properly installed, maintained, used for their intended purpose or under conditions which can reasonably be foreseen, and, where applicable, updated, and

(2) the processes put in place by the manufacturer comply with the essential requirements set out in Section 2 of Annex I.

CHAPTER II

OBLIGATIONS OF ECONOMIC OPERATORS

Commented [SŽ80]: LV: The obligations of economic operators must be proportionate, need to avoid duplication with obligations set out in other regulations, such as reporting on vulnerabilities and incidents, which are also regulated in the NIS2 directive.

Article 10

Obligations of manufacturers

1. When placing a product with digital elements on the market, manufacturers shall ensure that it has been designed, developed and produced in accordance with the essential requirements set out in Section 1 of Annex I.

2. For the purposes of complying with the obligation laid down in paragraph 1, manufacturers shall undertake an assessment of the cybersecurity risks associated with a product with digital elements and take the outcome of that assessment into account during the planning, design, development, production, delivery and maintenance phases of the product with digital elements with a view to minimising cybersecurity risks, preventing security incidents and minimising the impacts of such incidents, including in relation to the health and safety of users.

3. When placing a product with digital elements on the market, the manufacturer shall include a cybersecurity risk assessment in the technical documentation as set out in Article 23 and Annex V. For products with digital elements referred to in Articles 8 and 24(4) that are also subject to other Union acts, the cybersecurity risk assessment may be part of the risk assessment required by those respective Union acts. Where certain essential requirements are not applicable to the marketed product with digital elements, the manufacturer shall include a clear justification in that documentation.

4. For the purposes of complying with the obligation laid down in paragraph 1, manufacturers shall exercise due diligence when integrating components sourced from third parties in products with digital elements. They shall ensure that such components do not compromise the security of the product with digital elements.

5. The manufacturer shall systematically document, in a manner that is proportionate to the nature and the cybersecurity risks, relevant cybersecurity aspects concerning the product with digital elements, including vulnerabilities they become aware of and any relevant information provided by third parties, and, where applicable, update the risk assessment of the product.

6. When placing a product with digital elements on the market, and for the expected product lifetime or for a period of five years from the placing of the product on the market, whichever is shorter, manufacturers shall ensure that vulnerabilities of that product are handled effectively and in accordance with the essential requirements set out in Section 2 of Annex I.

   Manufacturers shall have appropriate policies and procedures, including coordinated vulnerability disclosure policies, referred to in Section 2, point (5), of Annex I, to process and remediate potential vulnerabilities in the product with digital elements reported from internal or external sources.

7. Before placing a product with digital elements on the market, manufacturers shall draw up the technical documentation referred to in Article 23.

   They shall carry out the chosen conformity assessment procedures referred to in Article 24 or have them carried out.

   Where compliance of the product with digital elements with the essential requirements set out in Section 1 of Annex I and of the processes put in place by the manufacturer with the essential requirements set out in Section 2 of Annex I has been demonstrated by that conformity assessment procedure, manufacturers shall draw up the EU declaration of conformity in accordance with Article 20 and affix the CE marking in accordance with Article 22.

8. Manufacturers shall keep the technical documentation and the EU declaration of conformity, where relevant, at the disposal of the market surveillance authorities for ten years after the product with digital elements has been placed on the market.

9. Manufacturers shall ensure that procedures are in place for products with digital elements that are part of a series of production to remain in conformity. The manufacturer shall adequately take into account changes in the development and production process or in the design or characteristics of the product with digital elements and changes in the harmonised standards, European cybersecurity certification schemes or the common specifications referred to in Article 19 by reference to which the conformity of the product with digital elements is declared or by application of which its conformity is verified.

10. Manufacturers shall ensure that products with digital elements are accompanied by the information and instructions set out in Annex II, in an electronic or physical form. Such information and instructions shall be in a language which can be easily understood by users. They shall be clear, understandable, intelligible and legible. They shall allow for a secure installation, operation and use of the products with digital elements.

11. Manufacturers shall either provide the EU declaration of conformity with the product with digital elements or include in the instructions and information set out in Annex II the internet address at which the EU declaration of conformity can be accessed.

12. From the placing on the market and for the expected product lifetime or for a period of five years after the placing on the market of a product with digital elements, whichever is shorter, manufacturers who know or have reason to believe that the product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential requirements set out in Annex I shall immediately take the corrective measures necessary to bring that product with digital elements or the manufacturer's processes into conformity, to withdraw or to recall the product, as appropriate.

Commented [SŽ81]: LV: More detailed explanation and reasoning would be necessary for the 5-year term, especially, taking into account that within the scope of the regulatory framework are both household and IoT products, for which the expected duration of operation is more than 5 years – e.g., industrial production, substance storage facilities and complexes. Also, sustainable development principles regarding product sustainability should be taken into account.

13. Manufacturers shall, further to a reasoned request from a market surveillance authority, provide that authority, in a language which can be easily understood by it, with all the information and documentation, in paper or electronic form, necessary to demonstrate the conformity of the product with digital elements and of the processes put in place by the manufacturer with the essential requirements set out in Annex I. They shall cooperate with that authority, at its request, on any measures taken to eliminate the cybersecurity risks posed by the product with digital elements, which they have placed on the market.

14. A manufacturer that ceases its operations and, as a result, is not able to comply with the obligations laid down in this Regulation shall inform, before the cease of operation takes effect, the relevant market surveillance authorities about this situation, as well as, by any means available and to the extent possible, the users of the concerned products with digital elements placed on the market.

15. The Commission may, by means of implementing acts, specify the format and elements of the software bill of materials set out in Section 2, point (1), of Annex I. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2).

Article 11

Reporting obligations of manufacturers

1. The manufacturer shall, without undue delay and in any event within 24 hours of becoming aware of it, notify to ENISA any actively exploited vulnerability contained in the product with digital elements. The notification shall include details concerning that vulnerability and, where applicable, any corrective or mitigating measures taken. ENISA shall, without undue delay, unless for justified cybersecurity risk-related grounds, forward the notification to the CSIRT designated for the purposes of coordinated vulnerability disclosure in accordance with Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] of Member States concerned upon receipt and inform the market surveillance authority about the notified vulnerability.

2. The manufacturer shall, without undue delay and in any event within 24 hours of becoming aware of it, notify to ENISA any incident having impact on the security of the product with digital elements. ENISA shall, without undue delay, unless for justified cybersecurity risk-related grounds, forward the notifications to the single point of contact designated in accordance with Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] of the Member States concerned and inform the market surveillance authority about the notified incidents. The incident notification shall include information on the severity and impact of the incident and, where applicable, indicate whether the manufacturer suspects the incident to be caused by unlawful or malicious acts or considers it to have a cross-border impact.

3. ENISA shall submit to the European cyber crisis liaison organisation network (EU-CyCLONe) established by Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] information notified pursuant to paragraphs 1 and 2 if such information is relevant for the coordinated management of large-scale cybersecurity incidents and crises at an operational level.

4. The manufacturer shall inform, without undue delay and after becoming aware, the users of the product with digital elements about the incident and, where necessary, about corrective measures that the user can deploy to mitigate the impact of the incident.

Commented [SŽ82]: LV: 1) There is a need to balance the implementation of the scope and modalities of the transmission of information, including the information that needs to be provided to ENISA in order to avoid a large amount of information that could not be processed and verified by the relevant authorities.
2) It is important that appropriated resources are planned for ENISA to cover new tasks and responsibilities. We suggest consult with ENISA, how they see impact of new tasks and resources available.
3) It is important to identify and reduce potential risks from vulnerability disclosure procedures established by this Article. We encourage to carry out a risk assessment.

5. The Commission may, by means of implementing acts, specify further the type of information, format and procedure of the notifications submitted pursuant to paragraphs 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2).

6. ENISA, on the basis of the notifications received pursuant to paragraphs 1 and 2, shall prepare a biennial technical report on emerging trends regarding cybersecurity risks in products with digital elements and submit it to the Cooperation Group referred to in Article [Article X] of Directive [Directive XXX/XXXX (NIS2)]. The first such report shall be submitted within 24 months after the obligations laid down in paragraphs 1 and 2 start applying.

7. Manufacturers shall, upon identifying a vulnerability in a component, including in an open source component, which is integrated in the product with digital elements, report the vulnerability to the person or entity maintaining the component.

Article 12

Authorised representatives

1. A manufacturer may appoint an authorised representative by a written mandate.

2. The obligations laid down in Article 10(1) to (7) first indent and (9) shall not form part of the authorised representative's mandate.

3. An authorised representative shall perform the tasks specified in the mandate received from the manufacturer. The mandate shall allow the authorised representative to do at least the following:

   (a) keep the EU declaration of conformity referred to in Article 20 and the technical documentation referred to in Article 23 at the disposal of the market surveillance authorities for ten years after the product with digital elements has been placed on the market;

   (b) further to a reasoned request from a market surveillance authority, provide that authority with all the information and documentation necessary to demonstrate the conformity of the product with digital elements;

   (c) cooperate with the market surveillance authorities, at their request, on any action taken to eliminate the risks posed by a product with digital elements covered by the authorised representative's mandate.

Commented [SŽ83]: LV: Need to check how this Paragraph corelates with Article 9, Point b of Cybersecurity Act (CSA). CSA norm sets requirement for ENISA to perform long term strategic analysis of cyber threats and incidents in order to identify emerging trends and help prevent incidents. It would be useful to consult with ENISA how CRA requirement fits in the reporting cycle.

Article 13

Obligations of importers

1. Importers shall only place on the market products with digital elements that comply with the essential requirements set out in Section 1 of Annex I and where the processes put in place by the manufacturer are compliant with the essential requirements set out in Section 2 of Annex I.

2. Before placing a product with digital elements on the market, importers shall ensure that:

   (a) the appropriate conformity assessment procedures referred to in Article 24 have been carried out by the manufacturer;

   (b) the manufacturer has drawn up the technical documentation;

   (c) the product with digital elements bears the CE marking referred to in Article 22 and is accompanied by the information and instructions for use as set out in Annex II.

3. Where an importer considers or has reason to believe that a product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential requirements set out in Annex I, the importer shall not place the product on the market until that product or the processes put in place by the manufacturer have been brought into conformity with the essential requirements set out in Annex I. Furthermore, where the product with digital elements presents a significant cybersecurity risk, the importer shall inform the manufacturer and the market surveillance authorities to that effect.

4. Importers shall indicate their name, registered trade name or registered trademark, the postal address and the email address at which they can be contacted on the product with digital elements or, where that is not possible, on its packaging or in a document accompanying the product with digital elements. The contact details shall be in a language easily understood by users and market surveillance authorities.

5. Importers shall ensure that the product with digital elements is accompanied by the instructions and information set out in Annex II in a language which can be easily understood by users.

6. Importers who know or have reason to believe that a product with digital elements, which they have placed on the market, or the processes put in place by its manufacturer, are not in conformity with the essential requirements set out in Annex I shall immediately take the corrective measures necessary to bring that product with digital elements or the processes put in place by its manufacturer into conformity with the essential requirements set out in Annex I, or to withdraw or recall the product, if appropriate.

   Upon identifying a vulnerability in the product with digital elements, importers shall inform the manufacturer without undue delay about that vulnerability. Furthermore, where the product with digital elements presents a significant cybersecurity risk, 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, giving details, in particular, of the non-conformity and of any corrective measures taken.

7. Importers shall, for ten years after the product with digital elements has been placed on the market, keep a copy of the EU declaration of conformity at the disposal of the market surveillance authorities and ensure that the technical documentation can be made available to those authorities, upon request.

8. Importers shall, further to a reasoned request from a market surveillance authority, provide it with all the information and documentation, in paper or electronic form, necessary to demonstrate the conformity of the product with digital elements with the essential requirements set out in Section 1 of Annex I as well as of the processes put in place by the manufacturer with the essential requirements set out in Section 2 of Annex I in a language that can be easily understood by that authority. They shall cooperate with that authority, at its request, on any measures taken to eliminate the cybersecurity risks posed by a product with digital elements, which they have placed on the market.

9. When the importer of a product with digital elements becomes aware that the manufacturer of that product ceased its operations and, as result, is not able to comply with the obligations laid down in this Regulation, the importer shall inform the relevant market surveillance authorities about this situation, as well as, by any means available and to the extent possible, the users of the products with digital elements placed on the market.

Article 14

Obligations of distributors

1. When making a product with digital elements available on the market, distributors shall act with due care in relation to the requirements of this Regulation.

2. Before making a product with digital elements available on the market, distributors shall verify that:

   (a) the product with digital elements bears the CE marking;

   (b) the manufacturer and the importer have complied with the obligations set out respectively in Articles 10(10), 10(11) and 13(4).

3. Where a distributor considers or has reason to believe that a product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential requirements set out in Annex I, the distributor shall not make the product with digital elements available on the market until that product or the processes put in place by the manufacturer have been brought into conformity. Furthermore, where the product with digital elements poses a significant cybersecurity risk, the distributor shall inform the manufacturer and the market surveillance authorities to that effect.

4. Distributors who know or have reason to believe that a product with digital elements, which they have made available on the market, or the processes put in place by its manufacturer are not in conformity with the essential requirements set out in Annex I shall make sure that the corrective measures necessary to bring that product with digital elements or the processes put in place by its manufacturer into conformity are taken, or to withdraw or recall the product, if appropriate.

   Upon identifying a vulnerability in the product with digital elements, distributors shall inform the manufacturer without undue delay about that vulnerability. Furthermore, where the product with digital elements presents a significant cybersecurity risk, distributors shall immediately inform the market surveillance authorities of the Member States in which they have made the product with digital elements available on the market to that effect, giving details, in particular, of the non-conformity and of any corrective measures taken.

5. Distributors shall, further to a reasoned request from a market surveillance authority, provide it with all the information and documentation, in paper or electronic form, necessary to demonstrate the conformity of the product with digital elements and the processes put in place by its manufacturer with the essential requirements set out in Annex I in a language that can be easily understood by that authority. They shall cooperate with that authority, at its request, on any measures taken to eliminate the cybersecurity risks posed by a product with digital elements, which they have made available on the market.

6. When the distributor of a product with digital elements becomes aware that the manufacturer of that product ceased its operations and, as result, is not able to comply with the obligations laid down in this Regulation, the distributor shall inform the relevant market surveillance authorities about this situation, as well as, by any means available and to the extent possible, the users of the products with digital elements placed on the market.

Article 15

Cases in which obligations of manufacturers apply to importers and distributors

An importer or distributor shall be considered a manufacturer for the purposes of this Regulation and shall be subject to the obligations of the manufacturer set out in Articles 10 and 11(1), (2), (4) and (7) where that importer or distributor 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 already placed on the market.

Article 16

Other cases in which obligations of manufacturers apply

A natural or legal person, other than the manufacturer, the importer or the distributor, that carries out a substantial modification of the product with digital elements shall be considered a manufacturer for the purposes of this Regulation.

That person shall be subject to the obligations of the manufacturer set out in Articles 10 and 11(1), (2), (4) and (7), for the part of the product that is affected by the substantial modification or, if the substantial modification has an impact on the cybersecurity of the product with digital elements as a whole, for the entire product.

Commented [SŽ84]: LV: A product whose part has been substantially modified will no longer correspond to the information specified in the technical documentation drawn up by the manufacturer of the original product, and these modifications will not be included in the tests carried out as part of the product conformity assessment procedure carried out in production. This in turn will mean that the product with its modified part will no longer be subject to the conformity assessment carried out for the original product and the product with the modified part will no longer be proven to comply with the essential requirements set out in all applicable regulatory acts. At the same time, the manufacturer of the original product will no longer be responsible for this new product with the modified part, since the modification of the product part was not intended on the part of original manufacturer.

Article 17

Identification of economic operators

1. Economic operators shall, on request and where the information is available, provide to the market surveillance authorities the following information:

   (a) name and address of any economic operator who has supplied them with a product with digital elements;

   (b) name and address of any economic operator to whom they have supplied a product with digital elements;

2. Economic operators shall be able to present the information referred to in paragraph 1 for ten years after they have been supplied with the product with digital elements and for ten years after they have supplied the product with digital elements.

ANNEX I

ESSENTIAL CYBERSECURITY REQUIREMENTS

5. Security requirements relating to the properties of products with digital elements

(1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks;

(2) Products with digital elements shall be delivered without any known exploitable vulnerabilities;

(3) On the basis of the risk assessment referred to in Article 10(2) and where applicable, products with digital elements shall:

(a) be delivered with a secure by default configuration, including the possibility to reset the product to its original state;

(b) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems;

(c) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms;

(d) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, as well as report on corruptions;

(e) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended use of the product (‘minimisation of data’);

(f) protect the availability of essential functions, including the resilience against and mitigation of denial of service attacks;

(g) minimise their own negative impact on the availability of services provided by other devices or networks;

(h) be designed, developed and produced to limit attack surfaces, including external interfaces;

(i) be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;

(j) provide security related information by recording and/or monitoring relevant internal activity, including the access to or modification of data, services or functions;

(k) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic updates and the notification of available updates to users.

6. Vulnerability handling requirements

Manufacturers of the products with digital elements shall:

(4) identify and document vulnerabilities and components contained in the product, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product;

(5) in relation to the risks posed to the products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates;

(6) apply effective and regular tests and reviews of the security of the product with digital elements;

(7) once a security update has been made available, publically disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and information helping users to remediate the vulnerabilities;

(8) put in place and enforce a policy on coordinated vulnerability disclosure;

(9) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;

(10) provide for mechanisms to securely distribute updates for products with digital elements to ensure that exploitable vulnerabilities are fixed or mitigated in a timely manner;

(11) ensure that, where security patches or updates are available to address identified security issues, they are disseminated without delay and free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.

ANNEX II

INFORMATION AND INSTRUCTIONS TO THE USER

As a minimum, the product with digital elements shall be accompanied by:

10. the name, registered trade name or registered trade mark of the manufacturer, and the postal address and the email address at which the manufacturer can be contacted, on the product or, where that is not possible, on its packaging or in a document accompanying the product;
11. the point of contact where information about cybersecurity vulnerabilities of the product can be reported and received;
12. the correct identification of the type, batch, version or serial number or other element allowing the identification of the product and the corresponding instructions and user information;
13. the intended use, including the security environment provided by the manufacturer, as well as the product's essential functionalities and information about the security properties;
14. any known or foreseeable circumstance, related to the use of the product with digital elements in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to significant cybersecurity risks;
15. if and, where applicable, where the software bill of materials can be accessed;
16. where applicable, the internet address at which the EU declaration of conformity can be accessed;
17. the type of technical security support offered by the manufacturer and until when it will be provided, at the very least until when users can expect to receive security updates;
18. detailed instructions or an internet address referring to such detailed instructions and information on:
    (a) the necessary measures during initial commissioning and throughout the lifetime of the product to ensure its secure use;
    (b) how changes to the product can affect the security of data;
    (c) how security-relevant updates can be installed;
    (d) the secure decommissioning of the product, including information on how user data can be securely removed.

HUNGARY

Hungarian written comments on the Cyber Resilience Act (CRA) for the second block that will be discussed at the Horizontal Working Party on Cyber Issues (HWP CI) on 1 February 2023.

Article 10 - Obligations of manufacturers

The draft Regulation has sections for consumer protection and user information in the justification and recital sections. We propose supplementing the draft with provisions regarding the obligation to provide simple and clear information to end users, similarly as it appears in the Finnish practice mentioned in the footnote in the proposal, also in regards to clear markings in similar ways to energy labels and environmental protection classification.

Article 10 - Obligations of manufacturers

(4) „For the purposes of complying with the obligation laid down in paragraph 1, manufacturers shall exercise due diligence when integrating components sourced from third parties in products with digital elements. They shall ensure that such components do not compromise the security of the product with digital elements."

In the first sentence of Article 10, paragraph (4) „*due diligence*" obligation is set out for the manufacturers, but in the second sentence of the same paragraph a more strict obligation of „*They shall ensure*" is set out. Due to the limited influence of manufacturers on the actual security of 3rd party components in digital supply chains, the obligation „*ensure*" should harmonized with the „*due diligence*" type obligation used in the first sentence.

Article 11 - Reporting obligations of manufacturers

According to regulations of Article 11 we would like to draw attention to the fact that the reporting procedures are not in line with regulations of NIS2 Directive [Article 12 and 23] and of Cybersecurity Act [mandate and tasks of ENISA in Cybersecurity Act (Article 4-9)].

With the implementation of NIS Directive a well-defined and well-functioning reporting procedure has been elaborated, and NIS2 directive also reserved it.

Article 23 of NIS2 Directive clearly states that essential and important entities notify, without undue delay, its CSIRT or, where applicable, its competent authority of any incident that has a significant impact on the provision of their services as referred to in paragraph 3 (significant incident).

And after that, where appropriate, and in particular where the significant incident concerns two or more Member States, the CSIRT, the competent authority or the single point of contact shall inform, without undue delay, the other affected Member States and ENISA.
However CRA doesn't regulate the same scope (manufacturers of product with digital elements) as NIS2 Directive (essential and important entities), we suggest not to duplicate the reporting obligations or to establish parallel reporting procedures, which could result uncertainty during the implementation and a slower reaction time to security incident.
Hungary suggests to preserve the same reporting procedure as defined in NIS 2 directive and modify Article 11 as well as recital (19) and (34)-(35).
We also suggest to specify the defintion „Member States concerned".

Article 11 - Reporting obligations of manufacturers

In Article 11, paragraph (6) we propose to consider changing the ENISA biennial reporting to annual reporting, since the basic data are mostly available in the ENISA weekly SAT reports, and cybersecurity trends can change significantly over a biennial period.

Article 12 - Authorised representatives

The draft Regulation foresees the designation of an authorised representative only as an option. In this context we would like to suggest that Article 4 (5) of the EU Market Surveillance Regulation ((EU) 2019/1020 of the European Parliament and the Council) should be amended to include this Regulation. This would ensure that there is an economic operator established in the European Union that market surveillance authorities may contact.

Annex I.

According to Annex I. 1. (3)(a) an option should be provided „to reset the product to its original state". This obligation may result in security risks, because the original state of the product may not contain all available security patches, and hence resetting the firmware to a previous, unpatched version may lead to a compromized product. If the product is reset not to its original state, but a default state with all security patches applied, it may secure the product from attacks.
(a) „be delivered with a secure by default configuration, including the possibility to reset the product to its original state;"
In order to overcome these kind of security risks, we propose to amend the text in the following way:

(a) „be delivered with a secure by default configuration, including the possibility to reset the product to its original state with all issued security patches installed;"

Recital (22)

The draft Regulation contains that for a modification to be considered "substantial" the modification must happen in a way "not foreseen by the manufacturer". This may be problematic in practice, because it would allow the interpretation that if a modification was "foreseen" by the manufacturer (eg the need to issue fixes for any security vulnerabilities in the future is foreseeable) then it would not count as "substantial" even if it impacted the compliance with the essential requirements. Therefore we suggest that the phrase "not foreseen by the manufacturer" by deleted. The manufacturer has to lay down in the technical documentation the features of the product, its intended use and the scope of the risk assessment conducted. Any modification that happens outside of this baseline and impacts the compliance with the essential requirements needs to count as "substantial". In addition we would like to remark that the last sentence of this preamble ("*As is the case for physical repairs or modifications, a product with digital elements should be considered as substantially modified by a software change where the software update modifies the original intended functions, type or performance of the product and these changes were not foreseen in the initial risk assessment, or the nature of the hazard has changed or the level of risk has increased because of the software update."*) should be moved to the main part of the Regulation due to its normative content.

Recital (32)

The second sentence ("*While manufacturers should comply with all essential requirements related to vulnerability handling and ensure that all their products are delivered without any known exploitable vulnerabilities, they should determine which other essential requirements related to the product properties are relevant for the concerned type of product.*") is ambiguous and hard to understand. We suggest the following alternative:

„All manufacturers should comply with all essential requirements related to vulnerability handling. Manufacturers ensure that all their products are placed on the market without any known exploitable vulnerabilities. Manufacturers should determine which other essential requirements related to the product properties are relevant for the concerned type of product."

NETHERLANDS

The Netherlands (NL) Written Comments Cyber Resilience Act (CRA)

Concerns: articles 1 – 5, 10 – 17, corresponding recitals and Annexes I and II

Horizontal Working Party on Cyber Issues (HWPCI)

20 January 2022

The Netherlands (NL) would like to thank the Swedish Presidency for the opportunity to provide written comments on all relevant provisions in the Cyber Resilience Act (CRA) concerning the general provisions, scope and obligations of economic operators and essential requirements.

We also would like to request renewed attention for Dutch written comments that were previously shared with the Swedish and Czech Presidencies.

As the Netherlands is still scrutinising the proposal, we may still provide additional or adapt earlier positions on the scope of the CRA.

Recital 10

We think that recital 10 needs further clarification on when exactly Open Source software becomes part of a commercial activity, to avoid uncertainty on who is responsible. We therefore propose the following for recital 10:

> (10) In order not to hamper innovation or research, free and open-source software developed or supplied outside the course of a commercial activity ***and therefore not 'made available on the market'*** ~~should~~ ***will*** not be covered by this Regulation. This is in particular the case for software, including its source code and modified versions, that is openly shared and freely accessible, usable, modifiable and redistributable. In the context of software, a commercial activity might be characterized not only by charging a price for a product, but also by charging a price for technical support services, by providing a software platform through which the manufacturer monetises other services, or by the use of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software.

The Netherlands is currently still working on text proposals to further clarify what non-commercial means in this context.

Article 3 - definitions

The Netherlands supports maximal adjustment of the definitions to the New Legislative Framework. Therefore, the Netherlands supports the additions proposed by the Swedish Presidency to article 3.

Synchronisation with NIS2 and the CSA is important, for instance when defining incidents.

Article 10 – Expected product lifetime

Our key concern pertains to the period of time in which manufacturers are required to guarantee the cybersecurity of their products, the expected product lifetime.

10(6) – 'expected product lifetime'

For the Netherlands a five year maximum period for manufacturers to guarantee the cybersecurity of products is not in line with what users could reasonably expect from most products with digital elements. Even as a minimum period of time, 5 years would not be sufficient in many cases. Many products should be relied on for much longer than five years. Industrial control systems should be relied on for at least ten or twenty years. The proposed 5 year maximum duration would therefore create the situation in which users will keep using a digital product that is no longer cybersecure. Because they are not aware that their product is no longer cybersecure or because they are not able to switch products (dependency). This would not be benificial to the main goal of the CRA. Moreover it would create a negative incentive for producers to put products on the market with only limited sustainability: no more than five years. We therefore propose to delete the mention of a 'maximum' period of time in relation to the expected product lifetime.

Additionally, the Netherlands proposes to give more guidance in article 10 para 6 on how the expected product lifetime should be determined for a product or category of products. If this would be purely left to the choice of the manufacturer, this could potentially undermine the effectiveness of the regulation.

Inspiration for a more prescriptive wording can be found in the digital content and digital services directives (Directive (EU) 2019/770 and Directive (EU) 2019/771). This states that the consumer should be supplied with security updates for the period of time "that the consumer may reasonably expect given the type and purpose of the goods and the digital elements, and taking into account the circumstances and nature of the contract".

We propose the following wording of article 10 para 6:

> "When placing a product with digital elements on the market, and for the expected product lifetime ~~or for a period of five years from the placing of the product on the market, whichever is shorter~~, manufacturers shall ensure that vulnerabilities of that product are handled effectively and in accordance with the essential requirements set out in Section 2 of Annex I.

When determining the expected product lifetime the manufacturers shall take into account the period of time, starting from the making available of the product on the market, the user may reasonably expect to use the product with digital elements, given the type and purpose of the product with digital elements. [*this could be combined with minimum periods per category of products, e.g. a minimum of 5 years for consumer products and a minimum of 10 years for industrial products*]

Manufacturers shall have appropriate policies and procedures, including coordinated vulnerability disclosure policies, referred to in Section 2, point (5), of Annex I, to process and remediate potential vulnerabilities in the product with digital elements reported from internal or external sources."

- Users should be clearly informed about the expected product lifetime before purchasing the product with digital elements, to enable users to take this into account when comparing products. This could be an extra incentive for manufacturers to use a realistic period.

Art.10**(10a): Manufacturers shall ensure that the products with digital elements or their packaging clearly and understandably indicate the end date for the expected product lifetime as mentioned in para 6, including at least the month and year, until which the manufacturer commits to ensuring the handling of vulnerabilities in accordance with the essential requirements set out in Section 2 of Annex I.**

We propose that a similar obligation will be included for imported products in article 13, and moreover would like to ask for more clarity in the wording of article 13 that the obligation to ensure the cybersecurity of products during the expected product lifetime in article 10 (6) will also be in place for imported products.

Article 11 - Reporting obligations

- The efficient reporting of incidents and vulnerabilities is an important element for the Netherlands. The Netherlands recognizes the added value a central EU-reporting desk for cyber security vulnerabilities and incidents of digital products may have, so that manufacturers do not have to report in all 27 Member States.
- As the Netherlands is still working on its position regarding the reporting obligations, for the further implementation of such a central reporting desk, we would be interested to explore possibilities for using (secure) automated processes.
- The in Article 11 proposed structure for reporting obligations would require 24/7 availability of ENISA and in this context, we have concerns about ENISA's role, procedures and resources. If it would become ENISA functioning as such a central reporting desk, the Netherlands would require further specification and definition of roles, responsibilities and procedures in the article text.

11(1)

- As 'active abuse' can be interpreted differently by different organizations (e.g. manufacturers, CERTs, researchers, intel suppliers), the Netherlands pledges for further specification of the definition, as described in Art. 3, sub 39, of 'actively exploited vulnerability', and to oblige the manufacturer to include details of the observed active exploitation in the reporting procedure. This information will help a CERT to perform a better risk assessment.
- The Netherlands considers it is in the interest of ensuring a high level of cybersecurity that manufacturers will have the possibility to **voluntarily** report vulnerabilities, especially those with a potential high-risk, for which active exploitation has not yet been observed. This offers national CERTs the opportunity to alert constituents to take mitigating measures before active abuse can take place.
- Manufacturers of critical products with digital elements (Annex III) should be required to report also vulnerabilities for which active exploitation have not yet been observed. In order to make this feasible and proportionate, the Netherlands is exploring options for an appropriate threshold value/risk classification.

11(3) forwarding reports to CYCLONe Network

- The Netherlands recommends that the decision whether reports are forwarded to the CYCLONe network should be made via the EU CSIRT network. The EU CSIRT network has the operational capabilities to assess vulnerabilities. As a result, Member States retain control over which CRA reports are considered as a large-scale cyber security incident and thus handled by the CYCLONE network.

We propose the following wording of article 11:

(1)

"(…) with digital elements. ***The manufacturer of critical products with digital elements (Annex III) shall in addition, without undue delay [and in any event within [...] of becoming aware of it], notify any vulnerability contained in the product with digital elements of which active exploitation has not yet been observed, based on thresholds as specified in […]. For all products with digital elements, the manufacturer shall have the possibility for voluntary reporting of vulnerabilities of which active exploitation have not yet been observed***. The notification shall include details concerning that vulnerability**, a description of the observed active exploitation** and, where applicable, any corrective or mitigating measures taken (…).

(3)

"~~ENISA~~ **The EU CSIRT-Network** shall submit to the European cyber crisis liaison organisation network (EUCyCLONe) established by Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] information notified pursuant to paragraphs 1 and 2 if such information is relevant for the coordinated management of large-scale cybersecurity incidents and crises at an operational level.

FINLAND

FI written comments on CRA proposal Block 2

Finland thanks the presidency for the clear progress schedule for the proposal and has the following comments on Block 2 texts. We do not comment on the recitals separately at this point because we see that they should be drafted accordingly with the changes in the articles.

Block 2

Art. 10 and recital 32

We think that the risk assessment is a critical part of the process given that all the cyber security measures of products are based on this assessment. Therefore it is important in order to reach the goals of the proposal. Common ground about the aspects of the assessment – even a general one - creates clarity for manufacturers but also may lead to more harmonized result.

We do recognize that risk assessment itself is done case by case where used technology and relevant security cases are evaluated in the context of a specific product and analysis should be done on a use case basis. Therefore, specific criteria for risk assessment in the legal text is not relevant.

However, we do think that some description of the topic could give some frame for this important topic and would like to suggest the following addition to article 10(2):

"3. When placing a product with digital elements on the market, the manufacturer shall include a cybersecurity risk assessment in the technical documentation as set out in Article 23 and Annex V. **The risk assessment should take into account [but not limit to] the intended and foreseeable use and conditions of use of the product including criticality of the product as listed in Annex III. Risk assessment should cover relevant cybersecurity threats and take into account the processed data, especially personal data.** For products with digital elements referred to in Articles 8 and 24(4) that are also subject to other Union acts, the cybersecurity risk assessment may be part of the risk assessment required by those respective Union acts. Where certain essential requirements are not applicable to the marketed product with digital elements, the manufacturer shall include a clear justification in that documentation."

For clarity, we think it also could be good to specifically mention that it is the responsibility of the manufacturer to determine the life cycle of the product. We suggest adding the following to Art. 10 (6):

"6. **The manufacturers shall determine the expected product lifetime in accordance with the normal and foreseeable use of the product.** When placing a product with digital elements on the market, and for the expected product lifetime or for a period of five years from the placing of the product on the market, whichever is shorter, manufacturers shall ensure that vulnerabilities of that product are handled effectively and in accordance with the essential requirements set out in Section 2 of Annex I."

We are open to discuss about the period of the lifecycle but we do see that the maximum time should be determined for proportionality reasons to the manufacturer. We have used the period of five years in Finnish Cybersecurity Label.

Art. 11 and recital 34

We would support changing the reporting obligations in line with NIS2-directive reporting requirements. We see that this would create more clarity for businesses when the reporting obligations are similar.

Art. 12

According to art 12 (2) obligations laid down in art. 10 (1)-(7) and (9) are not part of the authorised representative's mandate. However, art. 24 about conformity assessment procedures gives the impression that the conformity assessment could also be done by authorised representative instead of manufacturer. These articles are possibly contradictory with each other and it remains unclear if ensuring conformity can be part of the mandate of authorised representative or not.

When compared to the similar regulation in RED art 12 (1) this is not part of the mandate. This also seems to be the case for example in Artificial Intelligence Act that is still under negotiation. It gives the mandate to verify the conformity. We think that this should be clarified so that it is in line with other similar regulations.

Art. 13 and 14

Art 10(10) specifies that information and instructions should be either in electronic or physical form. Art. 13 (4) does not specify the format of the required information. This also reflects to Art. 14(2)(b) about the distributors obligation to check that everyone are fulfilling their obligations. It seems that the intention is that information of the importer should be physically available in a packaging – when there is one – but given that not all products do not have physical form it would be good to clarify that information could be given physically or electronically.

This might need more research since from consumer protection side the electronic format for instructions has not always been seen as sufficient.

Our stakeholders have raised a question concerning obligation of Art 13(6) and 14 (4) about the responsibility to bring the product to the manufacturers processes when they have reason to believe that they do not fulfill their essential requirements. At least in Finland the importers and distributors are fairly small actors compared to big importers and distributers in Europe and also compared to the big manufacturers. The fear is that with small importer or distributer, there is not enough leverage for big companies to get the corrective measures in process. Also, it might be a challenge for small businesses to analyze whether or not the products are in fulfilling the essential requirements or not.

Art. 16 and recital 22

We would like to make sure that the wording "for the purposes of this Regulation" does not cover modifications done for private purposes or research and development purposes i.e. it means that after modification there still needs to be "placing on the market" in order to the obligations to apply according to art. 16? This also reflects to the recital 22.

****

Something that we think needs further discussion is the role of online marketplaces and the obligations of their operators in the situation where a consumer buys a product from a vendor who sells the product in an online marketplace that is located outside of EU but the products could also be shipped to the EU. Online marketplace does not fit into the definition of economic operator. We think that this topic should be further examined also in the light of General Product Safety Regulation Chapter IV where these questions are taken into account.

Annex I

1 Security requirements

In general we need that there is a need for practical guidance for how to apply these requirements in practice. There are several points that need further clarification but may be more relevant to define in a practical guidance rather than part of the regulation.

Section 1
(3) (C) What is defined as state of the art mechanism? Does this also scale to the level of the assessed risk or is it fixed to some level?

As an addition, it would be good to require that product is should be easily and in a secure manner erased from the information of the user keeping in mind that it might be resold, recycled or disposed.

2. Vulnerability management

General question concerning handling vulnerabilities is that to what extent these requirements apply to third parties. It would be good to reach these requirements to whole supply chain in order to manage the vulnerabilities of the final product.

Annex II

We think that it is important to clearly express the length of the support period for the consumer in such a way that this factor can be assessed before buying the product.

Para 3 We think it would be beneficial also to require the manufacturer to separate different versions from another with different product numbers. Now sometimes can be found that different versions of same product may be identified as same even though the hardware inside for example might be different.

Recitals

(6) We would like to highlight also the risk based approach here so we would suggest adding the following to the text:

"(6) To increase the overall level of cybersecurity of all products with digital elements placed on the internal market, it is necessary to introduce objective-oriented and technology-neutral essential cybersecurity requirements for these products that apply horizontally **and are adapted risk based."**