Council of the European Union
General Secretariat

Interinstitutional files:
2022/0272 (COD)

Brussels, 07 February 2023

WK 843/2023 ADD 1

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.:	5806/23 15037/1/22 REV 1 12429/22 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: DE comments on Block 2

Delegations will find attached comments by the DE delegation on the revised Presidency compromise proposal as set out in 5806/23.

ANNEX

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.

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[1] when integrating components sourced from third parties ~~in products with digital elements~~ **in a manner that such components do not compromise the security of the product 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~~ **it** become**s** aware of and any relevant information provided by third parties, and, where applicable, update the **cybersecurity** 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,~~ **m**Manufacturers shall ensure**, when placing a product with digital elements on the market and for the declared support time ~~a period of time~~ after the placing on the market appropriate to the type of product and its expected lifetime,** that vulnerabilities of that product are handled effectively and in accordance with the essential requirements set out in Section 2 of Annex I.

Commented [TK1]: We support this proposed change

Commented [TK2]: It is unclear to us who according to this proposal will determine the "expected lifetime".

We propose to introduce the term "declared support-time" instead and state clearly that the declared support-time should in general be 5 years or more.

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. If this time exceeds the declared support-time, the manufacturer may also offer a longer free or paid support.

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.

[1] Recital to be added

Manufacturers shall determine the ~~period of time~~declared support time referred to in the first subparagraph of this paragraph taking into account the type of product, its expected lifetime and the time users reasonably expect to receive security updates given the product's functionality and intended purpose. For products with digital elements that have a lifetime of more than five years, the ~~period of time determined by the manufacturers~~declared support time referred to in the first subparagraph of this paragraph shall be no less than five years. The declared support time shall be appropriately longer than the time period determined by the design requirements for the type of product.

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.

Manufacturers shall specify, at the time of the placing on the market, in an easily accessible manner **and where applicable on the** packaging **of the product with digital elements, the month and year by which the technical security support, as referred in Annex II, point (8), ends.**

Security updates, referred to in Section 2, point (8), of Annex I, shall remain available for a minimum duration of ~~10 years~~the declared support time.

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.

Commented [TK3]: The product functionality and intended purpose should be linked to a type of product, as specified / intended in the first subparagraph (e.g. slow moving consumer goods).

Commented [TK4]: It is unclear to us who according to this proposal determins the length of the lifetime

Commented [TK5]: Industrial Control and Automation Systems (IACS) have a lifetime much longer than 5 years (>15 years). 5 Years is too fixed and short for products used in Critical Infrastructures. It needs to be made sure that the declared support time for products with longer expected lifetimes is appropriate.

Commented [TK6]: For example: In the Regulations for the dozens of product groups within the framework of the Eco Design Directive, several different applicable time periods for repair are stated. Therefore the declared support time of the CRA shall be longer than these. Otherwise the consumer would have the right to repair (for example the hardware/ a physical product with digital elements) but the product could then lack security support after the repair. This is especially important to ensure coherence with other EU legislation.

Commented [TK7]: According to the NLF it maintains the only task of the manufacturer to carry out the conformity assessment.

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 the requirements of 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 **provided** 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 on the market or putting into service of a product with digital elements.

12. From the placing on the market and for the **period of time referred to in paragraph 6** ~~**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 [TK8]: We support this proposed change.

Commented [TK9]: We support this proposed change

Commented [TK10]: The higlighted part must be reworded according to Article R2 of Decision 768/2008/EC.

Commented [TK11]: NLF alignment accoring to Article R2 of Decision 768/2008/EC

Commented [TK12]: User shall be able to recognise that information and instructions before the purchase decision.

Commented [TK13]: 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 [TK14]: Please cf. remarks to para 6.

13. Manufacturers shall, further to a reasoned request from a ~~market surveillance~~competent national 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 the CSIRTs designated as coordinators for the purposes of coordinated vulnerability disclosure ~~in accordance with~~pursuant to Article ~~[Article X]~~ 12(1) of Directive ~~[Directive XXX/XXXX (NIS2)]~~(EU) 2022/2555 of Member States concerned [through a single reporting platform] ~~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 or mitigating measures taken. Adding a notification to the reporting platform by the vendor will automatically inform CSIRTs, ENISA.

Commented [TK15]: NLF Alignment according to R2 of Decision 768/2008/EC

Commented [TK16]: We would prefer an electronic form for the national competent authority

Commented [TK17]: For the purpose of a better reading this should be the para 7.

Commented [TK18]: 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 [TK19]: 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 [TK20]: 24 hours might be too short for a diligent analsysis of a vulnerability

Commented [TK21]: A definition of "Member States concerned" is necessary. How would the manufacturer determine which CSIRTS to inform and which not.

Commented [TK22]: There is a single reporting platform but the report of a vendor will only be visible to one CSIRT, even if the vulnerability is actively exploited and that CSIRT may choose not to inform ENISA or other member states. Every CSIRT should see information about actively exploited products as soon as possible. Any delay or not telling other Member States is negligent and should not be allowed.

Commented [TK23]: The new reporting route would be from manufacturers via member states to ENISA. The former version described a mechanism from the manufacturer via ENISA to the member states. Both (challenging) mechanisms have their pros and cons and their practical implementation is unclear at the moment (also taking into account criteria like efficacy, available resources etc.). We see no benefit in prioritizing ENISA over CSIRTs or vice versa.
If there is a single reporting platform but the report of a vendor will only be visible to one CSIRT, even if the vulnerability is actively exploited and that CSIRT may choose not to inform ENISA or other member states. Every CSIRT should see information about actively exploited products as soon as possible. Any delay or not telling other Member States is negligent and should not be allowed.

Commented [TK24]: « 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

ENISA ~~**The CSIRTs** shall, without undue delay, unless for **justified** cybersecurity risk-related grounds, forward the notification to **ENISA** **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 authori**ties of all the concerned Member States** ~~**y**~~ about the notified vulnerability.

(1a) The manufacturer shall, without undue delay and in any event within 5 business days of becoming aware of it, notify to the CSIRTs designated as coordinators for the purposes of coordinated vulnerability disclosure pursuant to Article 12(1) of Directive (EU) 2022/2555 of Member States concerned [through a single reporting platform] any vulnerability contained in the product with digital elements. The notification shall include technical details concerning that vulnerability and, where applicable, any corrective or mitigating measures taken. Adding a notification to the reporting platform by the vendor will automatically inform CSIRTs, ENISA and inform the market surveillance authorities of all the concerned Member States 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**~~ **the single point of contact designated or established** ~~**in accordance with**~~ **pursuant to Article** ~~**[Article X]**~~**8(3) of Directive (EU) 2022/2555** ~~**[Directive XXX/XXXX (NIS2)]**~~ **of the Member States concerned [through a single reporting platform]** any incident[2] having impact on the security of the product with digital elements. ~~**ENISA**~~**The** ~~**designated**~~ **single point of contact** 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 authori**ties in all concerned Member States** 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.

[2] Definition will be added

Commented [TK25]: Proposed change to enhance resilience of products and effectiveness of market surveillance: add non exploited vulnerabilities - otherwise no information about inherent vulnerabilities would be submitted (which is the majority). Worst case scenario: having a product with hundreds of vulnerabilities and the manufacturer does not now that one of them is actively exploited: nothing is reported.
A shared platform is paramount to process the expected amount of data. Information about vulnerabilities and patches has to be submitted in a standardized way like VEX in CSAF-Standard.

Commented [TK26]: This will probably lead to double notifications with NIS2.

Commented [TK27]: Single Point of contact is only defined per Member State, 10(1) states to inform all CSIRTS in Member states concerned – which Member State will coordinate further the forwarding of information to ENISA and market surveillance authorities concerned? How is this state chosen, if this is not done via the single reporting platform?
If every CSIRT concerned informs every market surveillance authorities in all concerned Member States this would create lots of double communication

Commented [TK28]: The notification of « any incident » could overwhelm the authority. Maybe the term of « significant incident » according to NIS2 is better.

Commented [TK29]: Clarification of incident
HWP has to decide how an incident is defined. The proposed change distinguishes between vulnerability, actively exploited vulnerability and a compromise of the company which might impair the products (like backdoors in solarwinds).

Incident: a successful attack on the manufacturer that might have an impact on the security of the digital element

Commented [TK30]: What would be the « cybersecurity risk-related grounds » ?

3. ENISA shall submit to the European cyber crisis liaison organisation network (EU-CyCLONe) established ~~by~~**under** Article ~~[Article X]~~**16** of Directive **(EU) 2022/2555** ~~[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 [TK31]: 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).

Commented [TK32]: 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.

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**~~**established under** Article ~~[Article X]~~ **14** of Directive **(EU) 2022/2555**~~[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.

Commented [TK33]: It would be good if the vulnerability discovered by the manufacturer would be reported to the single reporting platform and not only to the open source maintainer

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 **cybersecurity** 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.

Commented [TK34]: As discussed in the HWP meeting on 1. Feb 23, we request adding these words back into the para.

Commented [TK35]: This must be reworded according to R3 of Decision 768/2008/EC

Commented [TK36]: 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).

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.

Commented [TK37]: This paragrahp has to be shifted to paragraph (2) according to R4 of Decision 768/2008/EC.

4. Importers shall indicate their name, registered trade name or registered trademark, the postal address and **website**, ~~**the**~~ email address **or other digital contact** 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.

Commented [TK38]: We support this proposed change.

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~~competent national 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~~competent national 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~~ action 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~~competent national 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 [TK39]: The correct term is "competent national authorities" according to R4 of Decision 768/2008/EC.

Commented [TK40]: The correct word is "action" according to R4 of Decision 768/2008/EC.

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 **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.

   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~~national competent 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.

Commented [TK41]: 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 [TK42]: According to R5 of Decision 768/2008/EC this paragraph is part of paragraph (2).

Commented [TK43]: For instance CSAF could be used, please see also Article 11, para 1.

5. Distributors shall, further to a reasoned request from a ~~market surveillance~~national competent 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 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 [TK44]: In what respect? Please clarify.

Commented [TK45]: This part must be deleted, because every person who carries out a substantial modificiation becomes a manufacturer.

Commented [TK46]: 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.

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

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 enable 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 **cybersecurity** 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 or built-in vulnerabilities;

(a) be **placed on the market** 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');

Commented [TK47]: If vulnerabilities become known for a product that has been manufactured, but not yet placed on the market (e.g. because it is being transported from the manufacturing site to the EU), could this lead to cases where the manufacturer would be required to disassemble large amounts of already produced and packaged products in order to patch a vulnerability? If so, foreseeing a (mandatory) automated security update process upon first start up could be an alternative, avoiding the aforementioned costs.

Commented [TK48]: 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".

(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~~ enable** that vulnerabilities can be addressed through security updates, including, where applicable, through automatic updates 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.

(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.

~~(k)~~(n)

2. VULNERABILITY HANDLING REQUIREMENTS

Manufacturers of the products with digital elements shall:

(1) 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;

Commented [TK49]: Proposal to be more precise

Commented [TK50]: 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.

Commented [DN51]: 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.

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

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

(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 and **clear and user friendly** information helping users to remediate the vulnerabilities; For products that are no consumer products and cannot be updated automatically and fall under Chapter I, Article 6, 2 (b) of this regulation, a standardized , structured and easily automatically processable machine-readable format (e. g. CSAF 2.0, Common Security Advisory Framework) shall be used.

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

(6) 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;

(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;

(8) 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.

Commented [TK52]: 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 [TK53]: We support this proposed change

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.~~6. where applicable, the internet address at which the EU declaration of conformity can be accessed

~~8.~~7. 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 information shall be distinctive and accessible before the purchase decision.

Commented [TK54]: Referring to the targets of this CRA, 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 [TK55]: 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 [TK56]: Manufacturers should not be forced to make the software bill of materials publicly available.

Commented [TK57]: Provides information about the durability of products and therefore be visible in a distinctive way, before buying a product. Esp. for private users, it could have great impact on purchase decisions and act as competitive advantage for manufacturers.

Highly depending on type of vulnerability. Information should be specific to singular vulnerability and not made in general. Thus recommending a dynamic consumer information in the frame of a consumer labelling scheme (in addition to the CE marking).

~~9.~~ detailed and clear instructions and information in a user-friendly language, carried on the product or referred by an internet address leading to that kind of instructions and informatuon. They include ~~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.