Independent Retail Europe

COMMISSION PROPOSAL FOR A CYBER RESILIENCE ACT
- COMMENTS OF INDEPENDENT RETAIL EUROPE -

22 December 2022

Avenue des Gaulois 3 / box 3
B – 1040 Brussels

T + 32 2 732 46 60
@ info@independentretaileurope.eu

www.independentretaileurope.eu
Transparency Register : ID number 034546859-02

EXECUTIVE SUMMARY

Independent Retail Europe welcomes the Cyber Resilience Act, as it will help to achieve a higher level of cyber security for products with digital elements made available in the EU. In this context, retailers have important obligations to fulfil to ensure that they sell to consumers only products with are in conformity with these new cyber security requirements. We therefore particularly welcome the use in the Cyber Resilience Act of the model of 'distributors obligations' used in the EU product safety acquis.

However, we consider that:

- Article 14 (distributors obligations) is not fully coherent with similar obligations under the General Product Safety Regulation (GPSR), as it fails to incorporate the novelties introduced in the GPSR. This creates legal uncertainty for retailers.
- Article 14 should be clarified to ensure that it does not introduce obligations that go beyond what is under the control of distributors
- Article 14(6) should be deleted as it un-necessarily duplicates an obligation that is a responsibility of manufacturers.
- New provisions are needed to close a potential loophole that would allow products, which are not in conformity to be made available in the EU (i.e. for products sold by non-EU sellers through online marketplaces and for which there is no EU-based manufacturer or importer).

COMMENTS OF INDEPENDENT RETAIL EUROPE ON THE CYBER RESILIENCE ACT

1. Distributors' obligations (article 14) should better reflect their specific role in the supply chain and be coherent with similar obligations under the General Product Safety Regulation

Article 14 of the Cyber Resilience Act lists the key obligations that any distributor of products with digital elements must fulfil when making such products available in the EU. This article directly applies to the retailers (and wholesalers) of such products, and is largely inspired from the EU product safety acquis.

In principle we welcome the use of the structure of the EU product safety acquis (and the New Legislative Framework) to determine distributors' obligations, as it constitutes a clear, practicable framework. However, certain aspects introduced by article 14 are still incoherent with a more recent part of the acquis and raise concern in terms of legal certainty. They also seem to go beyond what is under retailers' control and capacities. Since distributors deal with a wide range of products, only part of which are connected products, it is important that the safety obligations for these different products are clear, practicable and consistent, to avoid errors.

a) Article 14 should introduce the same novelties on distributor' obligations that are incorporated in the General Product Safety Regulation (GPSR)

Article 14(1) of the Cyber Resilience Act provides that retailers should act with due care. This 'due care' formulation, although based on the New Legislative Framework for products is vague, and therefore does not provide legal certainty as to the extent of this obligation. The Commission and the co-legislators recognised this fact in their discussion over the GPSR, and changed the 'due care' formulation (contained in the previous product safety Directive) into a more explicit provision

explaining what 'due care' means for retailers: not to put in jeopardy a product's conformity while the product is under their responsibility (see article 11(2) GPSR). **Article 14(1) should therefore be rewritten in line with article 11(2) GPSR to ensure coherence of distributors' obligations and legal certainty for distributors/retailers.**

Article 14(3) and 14(4) of the Cyber Resilience Act also fail to incorporate an essential clarification as to the scope of distributors' obligation when they have 'reasons to believe' that a product with digital elements is not in conformity, which was introduced in the GPSR. Indeed, the GPSR (article 11(3) and 11(4)) clarified that **distributors must act "*on the basis of the information in their possession*".** This is an important clarification as to the scope of distributors' obligations that should also be incorporated in article 14(3) and 14(4) of the Cyber Resilience Act.

Moreover, article 14(3) and 14(4) of the Cyber Resilience Act fail to include an obligation for the distributor to inform the importer (when applicable) in case of a significant cyber-security risk (as provided similarly for product safety risk in article 11 of the GPSR). It is indeed important to ensure coherence between the notification processes, especially as importers play a key role by putting products on the market when there is no EU-based manufacturer.

Action proposed:

- ➔ Ensure coherence of distributors obligations between the Cyber Resilience Act and the product acquis by introducing in article 14(1), 14(3 and 14(4) of the Cyber Resilience Act the novelties used in the GSPR article 11(2)(3) and (4)
- ➔ These novelties include a detailed explanation of what is 'due care', a reference to the 'information in possession' of distributors and a reference to importers for notification purposes. – see proposal of amendment in annex.

b) Article 14 should not introduce obligations that go beyond what is under the control of distributors

Article 14(3) and 14(4) of the Cyber Resilience Act provide some obligations for distributors when they "*consider or have reasons to believe*" that a product with digital elements is not in conformity with the essential requirements set out in Annex I.

This formulation ("consider or have reasons to believe") is ambiguous. Distributors lack the expertise to assess themselves whether the security requirements set out in annex I are in practice met by a specific product. **The only possibility for distributors to ensure that a product they distribute is in conformity, is to ensure that the product concerned meets the requirements mentioned in article 14(2)**, meaning that they are accompanied by a declaration of conformity (which engages the liability of the manufacturer), bear the CE marking, and are accompanied by the correct information.

The GPSR acknowledged this situation (for product safety) and therefore clarified the equivalent distributor obligation in relation to the conformity of the product. **Article 14(3) and 14(4) of the Cyber Resilience Act should similarly be amended to ensure that the lack of conformity relates to Articles 10(10), 10(11) and 13(4), as these are the only elements under the control of the distributor.**

Lastly, article 14(4) second paragraph also adds a completely new obligation for distributors to inform manufacturers without delay when they identify a (cyber) vulnerability in the product with digital elements (that is not in conformity, and which they have already made available on the market). In practice, distributors/retailers will not 'test' products that have been placed on the market or have already been made available, and lack the technical expertise to identify such vulnerabilities. On all technical aspects of the products, they are fully dependent on the information provided by the manufacturer. **This sentence in article 14(4) second paragraph should be deleted, as it provides an obligation that distributors are incapable of fulfilling.**

Action proposed:

- ➔ In article 14(3) and 14(4): clarify that the scope of distributors' obligation concerns the lack of conformity of the product with article 10(10), 10(11) and 13(14), and not the lack of conformity with the essential requirements set out in Annex I. Mandatory Information referred in article 10(10), 10(11) and 13(14) are the only elements under the control of the distributor (which guarantee the conformity of the product). See proposal of amendment in annex.
- ➔ In article 14(4) second paragraph: delete the sentence "*Upon identifying a vulnerability in the product with digital elements, distributors shall inform the manufacturer without undue delay about that vulnerability*", as this goes beyond the sphere of competence of distributors. See proposal of amendment in annex.

c) Article 14(6) should not introduce a duplication of tasks for distributors which are a responsibility of manufacturers and importers

Article 14(6) provides that distributors shall inform the relevant market surveillance authorities and the users of products with digital elements, when they become aware that the manufacturer of that product ceased its operations and cannot comply with its legal obligations.

This obligation is disproportionate and unnecessary, as manufacturers and importers are already obliged to inform market surveillance authorities in such cases (see article 10(14) and 13(9)) due to their specific role in the supply chain. Moreover, it is not the role of distributors to 'police' manufacturers and importers. Also, distributors that have ceased a contractual relationship with a manufacturer will not become aware of such closure of activities, while it is unclear for how long after the sale of the product such obligation would apply. **Article 14(6) should be deleted to avoid a useless duplication of tasks.**

Action proposed:

- ➔ Delete article 14(6), as this is a duplication of obligations already applicable to manufacturers and importers, therefore unnecessary and disproportionate, and concerns situations that are not under the control of distributors. See proposal of amendment in annex.

2. The sale of products with digital elements from third-country sellers through marketplaces should be addressed

Unlike other recent product legislation (e.g. the GPSR, the Product Liability Directive or the Regulation on Ecodesign for Sustainable Product), the Cyber Resilience Act does not contain any provision in relation to the sale of products through online marketplaces. This is surprising, as many large online

marketplaces are known to facilitate the sale of non-compliant products by third-country traders for which there is no manufacturer, importer or authorised representative established in Europe.

This is a loophole, which would allow rogue traders from all over the world to massively sell (in the EU) products with digital elements that are not compliant with the Cyber Resilience Act (and its essential cybersecurity requirements). Such a situation would largely undermine the benefit of this legislation, harm consumers and create unfair competition with EU traders.

We therefore call on the co-legislator to close this loophole in the Cyber Resilience Act. To this end, provisions should be introduced to **recognise the role of online marketplaces and fulfilment service providers, and give them residual obligations when the manufacturer, the importer or the seller using the marketplace are not based in the EU**.

Action proposed

- ➔ Introduce residual obligations for online marketplaces and fulfilment service providers for cases where products with digital elements are sold (by a third-country trader) through an online marketplace and for which there is no EU based manufacturer or importer.

ANNEX: proposal of amendment to article 14 (Obligations of distributors)

Commission proposal	Amendment proposal
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. […] 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	**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***~~ ***ensure that, while the product is under their responsibility, storage or transport conditions do not jeopardize its conformity with Articles 10(10), 10(11) and 13(4).*** […] 3. Where a distributor considers or has reason to believe***, on the basis of the information in its possession,*** 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***~~ ***Articles 10(10), 10(11) and 13(4)***, 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 ***or the importer, as applicable,*** and the market surveillance authorities to that effect. 4. Distributors who know or have reason to believe***, on the basis of the information in its possession,*** 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***~~ ***Articles 10(10), 10(11) and 13(4)***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. […]	~~***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. […]
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.	6. ***Delete***

Original version: English – Brussels, 22 December 2022