BEUC The European Consumer Organisation

The Consumer Voice in Europe

CYBER RESILIENCE ACT: TRILOGUE NEGOTIATIONS

BEUC recommendations

Contact: Cláudio Teixeira – digital@beuc.eu

BUREAU EUROPEEN DES UNIONS DE CONSOMMATEURS AISBL | DER EUROPÄISCHE VERBRAUCHERVERBAND
Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • www.twitter.com/beuc • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45

Co-funded by the European Union

Ref: BEUC-X-2023-128 -05/10/2023

Why it matters to consumers

Consumers expect the products they purchase to be safe and secure. However, the widespread use of connected products in our daily lives without sufficient cybersecurity protection has exposed consumers and made them vulnerable to serious cybersecurity risks. Cyberattacks on connected devices endanger consumers' privacy, security and physical safety. They can also lead to identity theft and cause economic damage. The EU must adopt a strong legal framework with clear rules for connected devices. The Cyber Resilience Act should deliver a higher level of protection for consumers, ensuring that connected products are secure by design and by default from the moment they are placed in the market and throughout their expected lifetime.

Summary

The European Commission proposed the Cyber Resilience Act (CRA) in September 2022.[1] In July 2023, both the Council[2] and the European Parliament[3] reached their respective positions, which led to the beginning of interinstitutional negotiations in September 2023.

Overall, BEUC welcomes the improvements suggested by co-legislators to the Commission proposal. For example, we welcome the Council position to introduce a clear risk methodology for high-risk products (Article 6), the proposal from Parliament to expand the list of critical devices to include consumer products (Annex III), or to strengthen consumer representation and redress, including the addition of the CRA to the Annex of the Representative Actions Directive (article 54a of the Parliament's position). This will allow consumers to collectively seek legal remedies.

However, there are aspects of significant concern which remain, notably the proposal from Council to reduce - instead of expand – the list of critical products in Annex III (enshrining the absence of consumer devices while removing essential products for internet security, such as internet routers) or the open question on whether manufacturers will be required to handle vulnerabilities and provide security updates throughout the expected lifetime of their products, or only for a limited support period (Article 10(6)).

BEUC calls on legislators to ensure that the CRA is fit for purpose and can fully deliver a high level of consumer protection. BEUC therefore makes the following recommendations:

1) **To broaden the scope with very limited exclusions and have clear definitions.**

- Co-legislators should expand and clarify that the CRA applies to relevant remote data processing solutions such as Software-as-a-Service when necessary for digital products to perform their functions, as per Council's position (Recitals 9. 9a).
- Co-legislators should refrain from any further exclusions from the scope, as per the Parliament's position (Article 2).

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0454
[2] https://data.consilium.europa.eu/doc/document/ST-11726-2023-INIT/en/pdf
[3] https://www.europarl.europa.eu/doceo/document/A-9-2023-0253_EN.pdf

- Co-legislators should follow the definitions proposed by the Council for 'consumer' (art. 3, 21a) as well as product 'recall' and 'withdrawal' (art. 3, 41, 42). The Council's proposal to delete the definitions of 'critical products with digital elements' and 'highly critical products with digital elements' (art. 3, 3-4), and the Parliament's proposal to introduce a definition of 'support period' should be rejected.

2) Manufacturers should monitor and address security vulnerabilities during a product's entire expected lifespan.

- Co-legislators should follow the Council's position to require manufacturers to monitor and address security vulnerabilities "for the expected product lifetime", instead of the Parliament proposal for a separate 'support period' (Article 10(6)).
- Co-legislators should add appropriate safeguards (e.g., clear criteria to follow, proactive monitoring role for market surveillance authorities), as proposed by Parliament's text in Recital 32a.
- In line with the Parliament's views, manufacturers should differentiate between security updates and functionality updates (Annex I (1) (3aa), Recital 32b).

3) The list of 'critical products' must be expanded and include consumer products.

- Co-legislators should support the Council's risk methodology to classify high-risk products (Article 6) under Annex III.
- The list of critical products (Classes I and II) must be extended to include consumer products, as proposed by the European Parliament.
- Co-legislators should introduce European cybersecurity certification schemes for all critical products as an alternative for proving conformity under the CRA.

4) Improving market surveillance and enforcement

- Co-legislators should return to the Commission's proposal on Article 11. They should keep the European Union Agency for Cybersecurity (ENISA) as the central reporting entity as per Parliament's position (art. 11(1)) and maintain the obligation for manufacturers to report "any" incident to ENISA, not just "significant" incidents as this would lead to legal uncertainty (art. 11(2) as per the Commission's proposal).
- Co-legislators should follow the Parliament proposal in Article 41 to empower ENISA to assist national authorities in technical aspects of investigations, by conducting assessments at the request of a national authority in form of non-binding opinions.

5) Strengthening consumer representation and redress.

- Co-legislators should follow the European Parliament's position to introduce:
    - a "single point of contact for users" (Article 11b).
    - require market surveillance authorities to introduce a mechanism to receive complaints from consumers (new article 41(8a)).
    - establish an "Expert Group on Cyber Resilience" (new article 6(a)).

6) Ensuring collective redress under the Representative Actions Directive

- Co-legislators should follow Article 54(1a) of the Parliament's text to add the CRA to Annex I of the Representative Actions Directive (RAD).

Contents

1. Broad scope with very limited exclusions and clear definitions

1.1. Scope (Article 2)

For the Cyber Resilience Act (CRA) to be effective, it requires a broad scope, where **any exclusions must remain strictly limited and adequately justified**. This is important to ensure that the CRA obligations apply to all relevant connected products which are still left without an adequate level of cybersecurity, putting users at risk on a daily basis.

BEUC generally **welcomes the European Parliament (EP)'s position to clarify the scope in Article 2**, including the clarifications on the application of the CRA to free and open-source software (when "made available on the market in the course of a commercial activity") and spare parts (excluding only those "exclusively manufactured to replace identical parts" and "supplied by the manufacturer").

We also welcome that the Council and the EP clarify that the CRA will also apply to products with digital elements "and their integrated remote data processing solutions" (Recitals 9, 9a). We also **support the Council's text in recital 9 to clarify that "Software-as-a-Service (SaaS) solutions constitute remote data processing solutions**" and should fall under the scope of the CRA insofar as they are essential for products to perform their functions. We also welcome the EP clarification that "for example, cloud enabled functionalities provided by the manufacturer of smart home devices that enable users to control the device at a distance, should fall within the scope of this Regulation" (recital 9). Such clarifications are instrumental to ensure that the CRA clearly includes software solutions such as Google Drive or Microsoft's SharePoint.

1.2. Definitions (Article 3)

BEUC welcomes the introduction by both Parliament and Council of the **definition of 'consumer' in Article 3**. In order to ensure full alignment with EU consumer law, we recommend **following the definition proposed by the Council**.

Furthermore, we welcome the clarification and alignment of the definitions of product 'recall' and 'withdrawal' (art. 3, (41) and (42)) in the Council's text with Regulation (EU) 2019/1020 on market surveillance and compliance of products.

However, **we oppose the Council's proposal to delete the definitions of 'critical products with digital elements' and 'highly critical products with digital elements'** from the Commission's text (art. 3, 3-4). It is fundamental that high-risk products listed in Annex III are clearly and conceptually identified. Adding to the legal uncertainty and conceptual confusion, the proposed change ultimately appears unnecessary, as the Council proposal maintains the current differentiation of products according to their levels of risk: the current listing of high-risk products in Annex III (critical products divided in Class I, Class II) remains in place, while certain 'highly critical products' which require stricter conformity assessment would still be listed apart (even if now on a new Annex III).

Moreover, **we do not support** the inclusion of **a new definition for a 'support period'** (art.3, 21c) as reflected in the Parliament's text. We strongly recommend co-legislators to replace this definition by sticking to the concept in the proposal of 'expected product lifetime'. We further explain how such a concept could contribute to undermine the objectives of the CRA and ultimately harm consumers in Section 2.2 of this paper.

BEUC recommendations

- Co-legislators should expand and clarify that the CRA applies to relevant remote data processing solutions such as 'Software-as-a-Service' when necessary for the digital products to perform its functions, as per Council's position (Recitals 9. 9a).

- Co-legislators should refrain from any further exclusions from the scope, as per the EP proposal (Article 2).

- Co-legislators should follow the definitions of 'consumer' (art. 3, 21a), 'recall' and 'withdrawal' proposed by the Council (art. 3, 41, 42). The Council's proposal to delete the definitions of 'critical products with digital elements' and 'highly critical products with digital elements' (art. 3, 3-4), as well as the Parliament's proposal to introduce a definition of 'support period' should be rejected.

2. Products should remain secure throughout their expected lifetime

2.1. 'Continuous conformity' for expected product lifetime, not only a few years (Article 10(6))

One of the key objectives of the Commission proposal is to ensure that consumer connected products are both **made secure and remain so** from the moment they are placed on the market for their expected lifetime. We welcome that the proposal includes mandatory requirements on the handling of cybersecurity vulnerabilities, effectively making manufacturers **responsible for the 'continuous conformity'** of the products that they place on the market, requiring them to **monitor and address vulnerabilities, and provide software updates**.[4]

For BEUC, the principle of 'continuous conformity' is fundamental: at the very least, manufacturers must be responsible for ensuring that the software of their products is adequately and regularly updated with vital system updates **throughout the expected product lifespan, and not only for a limited period of a few years.**

We therefore welcome the Council's proposal to amend Article 10(6) to require manufacturers to ensure vulnerability handling of their products **"for the expected product lifetime",** and no longer for a maximum limit of five years, as proposed by the Commission.

The Council position **significantly improves the Commission proposal by deleting the maximum limit of five years** for the provision of updates, an arbitrary limitation period which would effectively cap the provision of updates to all connected products covered by the CRA, regardless of their type, usage, or longevity.

Indeed, **the Cybersecurity Act (CSA) already enshrines this principle:** in article 46, the CSA determines that the European cybersecurity certification framework should ensure that products evaluated in accordance with EU certification schemes comply with specified security requirements "**throughout their life cycle**", while article 51 notes that security objectives of said schemes should "protect stored, transmitted or otherwise processed data" for a product's "**entire life cycle**".[5]

[4] Article 10(6) of the CRA proposal states that manufacturers have the obligation to handle the vulnerabilities of their products "for the expected product lifetime or for a period of five years from the placing of the product on the market, whichever is shorter".
[5] Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (Cybersecurity Act): https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

2.2. Proposal for separate "support period" would harm consumers (Article 10(6))

We are therefore **very concerned about the Parliament proposal in Article 10(6)** to introduce a new concept of a separate "support period" for the provision of updates. Unlike Council's proposal, the obligation for manufacturers to provide security updates would not be guided by the expected lifetime of a product: manufacturers would be responsible for determining a separate 'support period' for each product, which would only need to be 'proportionate' with the "expected product lifetime".

We strongly **advise against this proposal for the following reasons**:

- Firstly, a separate support period which is 'proportionate' to the expected product lifetime **would most likely be lower than the actual product lifetime**, as it incentivises manufacturers to set lower support periods.
- Secondly, there is a **direct correlation between the longevity of a product and the continuous provision of updates**, both in terms of functionality and security. When manufacturers cease to provide such updates, a **product's lifespan is artificially reduced:** without regular security updates, the product becomes unsafe to use; without functionality updates, the product becomes unable to perform essential functions and rapidly becomes obsolete.

BEUC member and UK consumer group Which? has found in several reports that **connected devices could be rendered obsolete as little as two years** after being placed on the market, should manufacturers choose to **stop providing vital software updates** [6] – even though 'smart' connected devices should have a greater life expectancy.[7]

We therefore recommend co-legislators to stick to the Council's definition of the "expected product lifetime" in the first instance.

2.3. Definition of 'expected lifetime' and appropriate safeguards (Article 10(6), Recital 32a)

However, we consider that the Council's position on how to define the "expected product lifetime" should also be improved. In particular, we regret that the Council allows manufacturers to determine this "expected product lifetime" **without sufficient safeguards being in place for consumer expectations**. The Council proposal to amend Article 10(6) requires manufacturers to "take into account the time users reasonably expect to be able to use the product […] given its functionality and intended purpose and therefore can expect to receive security updates".

This alone is insufficient. We recommend co-legislators to **complement the Council proposal with additional safeguards** to ensure that the "expected product lifetime" is adequately determined in line with consumer expectations and product-related criteria, as well as the most recent legislation on Ecodesign requirements.[8]

We therefore suggest that these **safeguards mirror the solutions already proposed by the Parliament position in article 10(6) and in Recital 32a**.

In these provisions, the Parliament proposed a set of safeguards which, although intended as a counterbalance to help determine a different 'support period', **would prove equally well suited** to ensure that manufacturers **determine the "expected lifetime" of their products in a fair and reasonable way**. Parliament's proposal for article 10(6) and in

[6] https://press.which.co.uk/whichpressreleases/smart-tvs-and-washing-machines-may-be-abandoned-by-brands-after-two-years-which-finds/
[7] https://press.which.co.uk/whichpressreleases/a-fridge-too-far-the-smart-appliances-that-cost-a-grand-more-but-may-only-last-two-years/
[8] Commission Regulation 2023/1670 on laying down Ecodesign requirements for smartphones, mobile phones other than smartphones, which states that software security updates for these products must be provided for a minimum of five years: http://data.europa.eu/eli/reg/2023/1670/oj

Recital 32a asks for additional safeguards in the form of **clearer criteria to guide manufacturers** in the determination of vulnerability handling periods, and **a stronger monitoring role for market surveillance authorities**, which would be required to "proactively ensure" that manufacturers determine these periods in a fair and adequate manner.

We therefore recommend that the **Council's proposal for Article 10(6) is complemented with the safeguards proposed by the Parliament's text in Article 10(6) and Recital 32a**.

BEUC recommended wording for a compromise on 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, ~~and for a period of time after the placing on the market appropriate to the type of and its,~~ that vulnerabilities of that product, including its components, are handled effectively **during the expected product lifetime** and in accordance with the essential requirements set out in Section 2 of Annex I.*
>
> *Manufacturers shall determine the expected product lifetime referred to in the first subparagraph of this paragraph ~~taking into account the time users reasonably expect to be able to use the product with digital elements given its functionality and intended purpose and therefore can expect to receive security updates~~. In doing so, the manufacturer shall ensure that the expected product lifetime is in line with consumer expectations, the nature of the product, the availability of the operating environment, **and that it adequately reflects the need to promote cybersecurity in the Union's market and is set with due consideration of the period during which a product with digital elements is expected to be available on the market.***
>
> ***Market surveillance authorities should proactively ensure that manufacturers apply these criteria in an adequate manner. Market surveillance authorities should collect and analyse data about the support periods set by manufacturers and the expected product lifetimes.** To that end, manufacturers shall make available **to** ~~upon request of~~ market surveillance authorities information considered in order to determine the duration of the ~~support period~~ **expected lifetime** for the product made available on the market. Market surveillance authorities shall monitor products with digital elements and ensure actively that manufacturers have applied these criteria in an adequate manner ~~including an assessment of the information received from the manufacturers on the expected product lifetime, when determining the support period~~. Where applicable, the ~~support period~~ **expected lifetime** shall be clearly stated on the product, its packaging ~~or~~ **and** be included in contractual agreements. In any case, end users shall also be informed before purchase of the duration of the ~~support period~~ **expected lifetime**.*

2.4. Software updates: unbundling security and functionality updates (Annex I)

The CRA should also deliver more transparency and differentiation regarding software updates. This is important because that has implications on the durability and functionality of products. We therefore **support the Parliament proposal** in Annex I (1) (3aa) and Recital 32b, to ensure that manufacturers are **obliged to differentiate between security updates** and **functionality updates**, establishing that these updates should be provided separately.

We also welcome the calls from Parliament (Annex I (1) (3ab), Recital 32b) and Council (Annex I (1) (3a), Recital 11a), for security updates to be installed automatically, provided that users have a clear opt-out mechanism, which effectively establishes a clear-cut operational differentiation between security and functionality updates.

BEUC recommendations

- Co-legislators should follow the Council in requiring manufacturers to monitor and address security vulnerabilities "for the expected product lifetime", rejecting the Parliament proposal for a separate 'support period' (Article 10(6)).

- Co-legislators should complement the Council's text in Article 10(6) with the safeguards proposed by Parliament in Recital 32a.

- In line with the European Parliament's position, manufacturers should differentiate between security and functionality updates (Annex I (1) (3aa), Recital 32b).

3. Critical products: high risk and consumer devices

3.1. A new risk methodology (Article 6)

BEUC recommends following the **Council's approach on Article 6, introducing a new risk methodology.** The Council establishes two criteria to determine which products should be considered critical products of higher risk. This criterion can prove instrumental to guide future updates of the list of critical products, such as the sensitivity of the data processed, the risks entailed by the normal use of a product or the potential dangers that these devices may represent in case of a successful cyberattack, including potential physical harm for consumers (e.g. damages to "the health and safety of a large number of individuals", Article 6(1) (a)).

3.2. Consumer products are also critical products (Annex III)

While the Council introduced a risk methodology, **the list of critical products in Annex III remains a closed list,** which requires to be updated by the Commission. It is fundamental to ensure that this list remains as broad and inclusive as possible, ensuring a broad starting point for the application of the CRA while providing the necessary legal certainty for manufacturers to start preparing for compliance.

We strongly oppose the Council's suggestion to delete most categories of critical products currently in Annex III. From the initial 38 categories of products in the Commission's proposal, only ten remain in the Council position. For instance, **browsers or password managers** have been deleted, despite how critical they are for internet and device security.[9]

BEUC strongly recommends that co-legislators **maintain but also expand the list of products** in the Commission's proposal. **We support the EP position on Annex III**, particularly in relation to the introduction of the following sensitive consumer products. We call on co-legislators to prioritise these product categories, in the following order:

[9] In August 2022, LastPass, one of the most popular password managers (25 million users worldwide), was hacked. A malicious actor had access to LastPass' development environment for four days. Although the company reported that no passwords were leaked, the attacker got access to LastPass' source code and technical information.

- **Smart toys and products for children,** e.g., toys relying on an active connection to function, baby monitors, educational devices and wearables for children. (Annex III, class I, 23c).
- **Home automation systems,** e.g., smart home servers, virtual assistants (Annex III, class I, 23a).
- **Security devices,** e.g., smart security alarms, smart smoke detectors or carbon monoxide alarms, digital door locks, security cameras and private surveillance equipment (Annex III, class I, 23b).
- **Personal health appliances and wearables,** e.g., fitness trackers, smart watches, panic buttons, wearables for minors (Annex III, class I, 23d).

BEUC members have **consistently exposed how critical vulnerabilities[10] in these devices can be easily exploited**.[11] Given their sensitive nature, such products can pose higher risks to consumers. When cyberattacked, they can harm user health and safety or adversely impact fundamental rights like privacy and data protection. Compromised devices with inbuilt audio or video hardware, health data monitoring or location software can pose **risks of surveillance, security breaching, violation of fundamental rights or putting health and safety on the line**.[12] Mitigating these risks requires such products to be submitted to a **stricter conformity assessment procedure**: their inclusion in the critical list is therefore essential to protect consumers from potential harm and to safeguard their rights.

For instance, **connected products for children** pose especially significant risks to consumers, given their unfettered access to the interior of the family home and their direct access to children. In 2016, BEUC's Norwegian member Forbrukerrådet demonstrated how a **connected doll named Cayla could become a real-life illegal spying device[13] and a risk to the safety of children**, finding that attackers could easily hack the toy from a distance and use it to directly speak to the children, thus putting their physical safety and privacy at risk.[14] Besides smart toys, other connected devices are also cause for concern. In 2017, Forbrukerrådet found very serious security flaws in smart watches for children: testing found that such products, enabling parents to contact and check their child's real-time location, could easily accessed by attackers, potentially allowing them to track and directly contact children or even alter the geo-location (location spoofing) of the watch.[15]

From the very beginning, the CRA proposal expressly recognised, in its Recital 8, the importance of "adopting cybersecurity requirements" for **"products intended for vulnerable consumers such as toys and baby monitors"**. Therefore, there can be no reason why such sensitive devices are not recognised as critical products.

---

[10] In 2018, BEUC's Belgian member Test-Achats (TA) launched the "Hackable Home" campaign, equipping, TA gave ethical hackers a week to take control of a home with a range of smart devices. Out of 19 connected appliances, half were vulnerable after just five days. In the case of the alarm systems, hackers were able to hack into the surveillance cameras to monitor its live feed from a distance, disconnect the alarm sensors and even mute smoke detectors. https://www.test-achats.be/hightech/smart-home/presse/la-securite-des-appareils-domestiques-intelligents-est-une-veritable-passoire

[11] In 2017, BEUC member Which? from the UK conducted a test with smart gadgets, including an internet router, wireless surveillance cameras, and children's toys. 8 out of 15 tested appliances included at least one security flaw. The hackers gained access to the internet router and the wireless home CCTV camera system, going as far as taking control and freely manoeuvre the wireless cameras of the house, being able to monitor all the activity inside the house. https://press.which.co.uk/whichpressreleases/the-hackable-home-investigation-exposes-vulnerability-of-smart-home-devices/

[12] The dangers of home automation systems, such as virtual assistants, have become clearer in 2021, when Alexa voice assistant by Amazon "challenged" a 10-year-old girl to touch a live power plug with a coin: https://www.bbc.com/news/technology-59810383

[13] Following a Cold War era legislation, Germany's Federal Network Agency (*Bundesnetzagentur or BNetzA*) classified Cayla as an "illegal espionage apparatus" and ordered parents to destroy or disable the toy, as it could be used to illegally spy on children. https://www.theguardian.com/world/2017/feb/17/german-parents-told-to-destroy-my-friend-cayla-doll-spy-on-children

[14] https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/

[15] https://fil.forbrukerradet.no/wp-content/uploads/2017/10/watchout-rapport-october-2017.pdf

In addition, security devices particularly stand out as an example of consumer devices which **should be considered as critical products**, as the hacking of security and alarm systems can reasonably be **expected to be driven by a criminal intent**.[16] Recently, in September 2023, BEUC's Belgian member Test Achats/Test Aankoop followed up on its 'Hackable Home' campaign, with its product testing once more revealing massive cybersecurity problems in consumer devices, especially in security cameras and digital door locks.[17] Only last year, the German Federal Office for Information Security (BSI) warned about a **faulty digital door lock with a critical vulnerability** that allowed nearby attackers to hack the radio signal door lock to gain illegal access to buildings. Despite eventually admitting to the vulnerabilities of this product, the manufacturer was ultimately unable to correct this vulnerability by updating this version or removing the product from the market.[18]

3.3. Covering components alone is not enough (Annex III)

We strongly oppose the **Council position on regulating high-risk consumer products**.

In Recital 8, the Council position recognises that "stricter conformity assessment procedure […] will contribute to prevent negative impacts of the exploitation of potential cybersecurity vulnerabilities on consumers", **but falls short of adding consumer products to Annex III**, arguing that "microprocessors, microcontrollers and general purpose operating systems, will typically be components that play an essential role for the cybersecurity of consumer products, including smart home products with safety functionalities, such as door locks and alarm systems, connected products for children, including toys and baby monitors, and wearable technology and other connected health devices."

This approach is insufficient to protect consumers from cybersecurity risks, as **a connected product is more than the sum of its parts**. While microprocessors and microcontrollers might be crucial components, they are not the only parts that play a key role in preventing cyberattacks. Cybersecurity in connected consumer products is a complex and multifaceted matter that involves multiple layers of protection. The Council's rationale raises concerns as it potentially **shifts the responsibility for ensuring products are inherently secure away from consumer product manufacturers** and onto other suppliers in the supply chain. This shift could lead to a lack of accountability and responsibility, leaving consumers and their data vulnerable.

The Council's reasoning also appears to downplay **the substantial role that manufacturers play in enhancing cybersecurity**. Manufacturers of consumer products contribute and add value through their design, development, and quality control processes. They are instrumental in addressing insecure practices and ensuring that products meet stringent safety and security standards. Consequently, downplaying their role may have unintended consequences for the overall product integrity and consumer protection. For instance, BEUC's UK member Which? found that users of connected devices such as speakers or washing machines are being asked to provide substantial amounts of data to manufacturers beyond than what is needed for a product to function, practices which could compromise users' privacy and personal data[19].

[16] https://www.which.co.uk/news/article/more-than-100000-wireless-security-cameras-in-the-uk-at-risk-of-being-hacked-a0vVp2v8zNqx
[17] https://www.test-achats.be/hightech/smart-home/dossier/hackers-appareils-connectes?isFromNewsletter=1
[18] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Warnungen-nach-P7_BSIG/2022/BSI_W-005-220810.pdf?__blob=publicationFile&v=12
[19] https://press.which.co.uk/whichpressreleases/spies-in-your-home-which-warns-of-security-camera-that-sends-data-to-tiktok-and-washing-machines-that-demand-to-know-your-age/

Responsibility for cybersecurity risks therefore goes beyond an individual component. **Manufacturers should be required to follow secure design and development practices by default** to minimise vulnerabilities from the outset, from firmware and software to user authentication and privacy protection.

3.4. Strengthening the conformity assessment for critical products (Article 24)

Although falling short of requiring all 'critical products' listed in Annex III to undergo a mandatory European cybersecurity certification, we welcome the amendments by both the Council and Parliament in Article 24(1) to introduce **European cybersecurity certification schemes** established under the Cybersecurity Act (CSA)[20], as a way of proving conformity with the CRA instead of relying on self-assessments.

In particular, we **welcome the Council proposal to introduce this conformity assessment possibility for products listed in both Class I and Class II of Annex III (art 24(2) and (3)),** as well as a new point 3aa where a new category of higher risk products (new Annex IIIa) would require a cybersecurity certification scheme by default.

At the very least, the CRA proposal should be fully aligned with the provisions of the CSA on this matter, making it clear that resorting to **self-assessment should not be considered for products which present a higher cybersecurity risk for consumers**.

BEUC recommendations:

- The CRA should include a risk assessment methodology as proposed by Council (Article 6).
- Co-legislators should follow the EP proposal to expand the list of critical products in Annex III and include key sensitive products for consumers such as smart toys.
- Co-legislators should introduce European cybersecurity certification schemes for all critical products as a way to prove conformity under the CRA.

4. Stronger market surveillance and enforcement

4.1. More effective incident reporting (Article 11)

BEUC recommends co-legislators to go back to the original principles of the European Commission's proposal in Article 11 to ensure a more effective incident reporting.

Article 11(1) should entrust ENISA as the central reporting entity. This is also part of the European Parliament's position.

Regarding article 11(2), we support **keeping in the final text the obligation to report "any incident"** with an impact on the security of a product, which is from the Commission's proposal (a position shared by Council). We strongly oppose the EP proposal, which limits reporting obligations to "significant" incidents. While Parliament introduces two criteria to determine what constitutes a "significant" incident, this would still lead to legal uncertainty and impact the effective application of the CRA.

For example, it is not clear what would constitute a "considerable" damage (Art. 11(2) (a), (b)). The quantification of harm is very difficult to assess and would require companies under cyberattack to carry out an exercise in foresight which authorities and courts are

[20] Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (Cybersecurity Act): https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

best placed to determine. Moreover, it could contribute to hinder the active reporting of vulnerabilities and contribute to keep vital information away from both authorities and consumers.

4.2. Improving market surveillance and enforcement (Article 41)

BEUC welcomes the amendments proposed by the co-legislators to improve the market surveillance and enforcement framework in Chapter V of the CRA proposal. In particular, **we support the EP text** which **strengthens and clarifies the role of national authorities to conduct effective market surveillance and sanction economic operators for non-compliance** with the requirements set out in the CRA. In addition, we welcome the EP position in Article 41, which confers a clear role on ENISA to support compliance with the CRA. ENISA should assist national authorities in the technical aspects of their investigations by conducting evaluations and assessments at the request of a national authority, in the form of non-binding opinions.

BEUC recommendations

- Co-legislators should return to the Commission's proposal on Article 11. They should keep the European Union Agency for Cybersecurity (ENISA) as the central reporting entity as per Parliament's position (art. 11(1)) and maintain the obligation for manufacturers to report "any" incident to ENISA, not just "significant" incidents as this would lead to legal uncertainty (art. 11(2) as per the Commission's proposal).

- Co-legislators should follow the Parliament proposal in Article 41 to empower ENISA to assist national authorities in technical aspects of investigations, by conducting assessments at the request of a national authority in the form of non-binding opinions.

5. Empowering consumers: representation and redress mechanisms

5.1. Effective redress mechanisms for consumers (Articles 11, 41)

BEUC **welcomes the European Parliament's position in Article 11b** to introduce a "**point of single contact for users**", a solution which privileges dialogue between consumers and manufacturers, allowing for swifter remedies for consumers. This article is based on the similar procedure of a "Single Point of Contact" adopted in Article 12 of the Digital Services Act (DSA). To ensure coherence between EU digital laws, we further recommend co-legislators to harmonise the terminology of this mechanism under the CRA with Article 12 of the DSA: "**single point of contact for users**".[21]

We also **support the European Parliament's proposal in article 41(8a)** to require market surveillance authorities to introduce a **mechanism to receive complaints from consumers.** Establishing an independent consumer complaint mechanism that is addressed to market surveillance authorities is crucial to allow consumers to directly report vulnerabilities, incidents, and cyber threats to authorities. It increases the sharing of information while allowing consumers a clear way to seek redress when all else fails.

[21] Regulation (EU) 2022/2065 on a Single Market for Digital Services (Digital Services Act), Article 12: http://data.europa.eu/eli/reg/2022/2065/oj

5.2. Increasing representation of consumer organisations (new Article 6a)

We support the **European Parliament's proposal for a new article 6(a) which instructs the Commission to establish an "Expert Group on Cyber Resilience"** which expressly includes civil society and consumer organisations. The importance of such an inclusive, representative body advising the Commission and taking an active role in the preparation of delegated acts (e.g., advising the Commission on amendments to the critical products list in Annex III) is a key improvement of this proposal.
This development could bring substantial **added value to the decision-making process,** by creating synergies and increasing transparency and accountability. From a consumer perspective, it is fundamental for consumer organisations, with a long track record in product testing and collecting key evidence on consumer products, to be able to provide their direct input to improve consumer protection.

BEUC recommendations

Co-legislators should follow the European Parliament's proposal to:

- introduce a "single point of contact for users" (Article 11b).
- require market surveillance authorities to introduce a mechanism to receive complaints from consumers (new article 41(8a)).
- establish an "Expert Group on Cyber Resilience" (new article 6(a)).

6. Addition of the CRA to the Representative Actions Directive's Annex I

We strongly welcome that both co-legislators agreed on the importance to include the CRA in Annex I of the Representative Actions Directive (RAD). [22] We recommend co-legislators to follow the Parliament's approach to introduce a single new Article 54a which adds the CRA to the Annex of the RAD, so consumers benefit from collective redress mechanisms and injunctive relief when harmed due to non-compliance with the obligations of the CRA. This will also ensure greater coherence with other recent EU digital and product safety laws (e.g., the Digital Services Act, Digital Markets Act, General Product Safety Regulation, Data Act) which have also been added to Annex I of the RAD.

BEUC has explained in more detail why the CRA needs to be added to the Annex I of the Representative Actions Directive in a position paper.

BEUC recommendation

- The CRA should be added to Annex I of the Representative Actions Directive, as per the Parliament's position (Article 54a).

[22] Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC: http://data.europa.eu/eli/dir/2020/1828/2023-05-02

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EISMEA. Neither the European Union nor the granting authority can be held responsible for them.