The Consumer Voice in Europe

THE CYBER RESILIENCE ACT PROPOSAL

BEUC position paper

Contact: Cláudio Teixeira – digital@beuc.eu

BUREAU EUROPÉEN 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-2023-006 -23/01/2023

Why it matters to consumers

The number of digital services and connected devices in consumers' lives is skyrocketing. Consumers expect the products they purchase to be safe and secure. Cyberattacks on connected devices put consumers at risk and endanger their privacy and security, even their physical safety. They can also lead to identity theft and cause economic damage. It is fundamental that the EU develops a strong legal framework to ensure that consumers are adequately protected and that connected devices are cybersecure.

Summary

BEUC – The European Consumer Organisation welcomes the European Commission proposal on the Cyber Resilience Act (CRA). This proposal answers a longstanding need that BEUC and its members have identified and warned about repeatedly. Over the past years, BEUC members have demonstrated that too many connected products sold on the European market lack even the most basic security features. Too many products are putting consumers at risk on a daily basis.

BEUC fully supports the proposed introduction of mandatory, essential cybersecurity requirements for manufacturers, distributors and importers of digital products and their ancillary services, to ensure that these products are secure by design and by default.

However, substantial improvements are still needed regarding several aspects of the proposal, to ensure that it is fit for purpose and can fully deliver a high level of protection to consumers.

In particular, BEUC makes the following key recommendations:

1) **A broader scope covering all types of digital products and associated services.**

- The new rules must be applicable to all connected products, and their associated services, marketed to/intended for consumers.
- The scope should be expanded to cover all web-based services (e.g. Software-as-a-Service, websites) available to consumers.

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

- Mandatory cybersecurity requirements for manufacturers on vulnerability handling should apply throughout the product's entire expected lifespan, and not be limited to a maximum period of five years.
- A threshold of five years to address vulnerabilities could eventually be a minimum limit, but not a maximum threshold.

3) The conformity assessment procedure must be strengthened.

- Third party assessment should be the rule to assess the conformity of 'critical products with digital elements' under Annex III.
- Self-assessment should only be allowed for those products which are not considered to be 'critical products with digital elements' under Annex III.
- Harmonised standards should only be used to define technical requirements, not to replace legal obligations and requirements.
- Reliance on harmonised technical standards should not open the door to self-assessment in the case of 'critical products with digital elements', even those belonging to Class I.

4) 'Critical products' must include consumer products and be subjected to mandatory cybersecurity certification

- The legislation should mandate cybersecurity certification level "high" for 'critical products with digital elements' listed in Annex III while discarding other options, especially those relying on self-assessment.
- The list of critical products (Classes I and II) must have a broader scope, going beyond its current focus solely on products intended for industrial use.
- In particular, the list of 'critical products with digital elements' of higher risk (Annex III, Class II) must also be extended to include consumer products.

5) The market surveillance and enforcement framework must be clarified and improved.

- Effectiveness and consistency of market surveillance and enforcement must be strengthened, by providing for cooperation mechanisms between all market actors.
- There must be clear cross-sector cooperation mechanisms for relevant supervisory authorities.
- A 'virtuous cycle' of cooperation between consumers and national authorities should be encouraged.
- Enforcement at the national level should be reinforced at a technical level. Beyond a supporting role to the investigation procedures of the European Commission, the CRA proposal should also establish an explicit role for ENISA to assist national authorities in their investigations, at their own request. An alternative would be to create a technical body for this role.

6) Effective remedies and means of redress for consumers when obligations are not respected.

- Consumers have a right to cybersecure products and services, and should have a clear right to complain to a national authority and access judicial remedies when they are affected by non-compliance with the CRA obligations.
- Manufacturers should be required to make a complaint mechanism available and be obliged to react to consumer complaints within a short period of time, with a maximum of five working days.
- Affected users should have the right to remedies/compensation in case they suffer damages caused by non-compliance with the CRA.

- Consumer organisations/civil society organisations should be able to represent individual consumers in the exercise of their rights.
- The CRA must be added to the Annex of the Representative Actions Directive (RAD) to enable collective redress actions and injunctions in case of mass harm.

Contents

1. Introduction

On 15 September 2022, the European Commission published the proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements ('Cyber Resilience Act').[1]

BEUC – The European Consumer Organisation welcomes the Cyber Resilience Act (CRA) proposal and its objective to introduce new horizontal EU rules to improve cybersecurity protection of connected products. The CRA establishes mandatory and essential cybersecurity requirements for manufacturers of products with digital elements and their ancillary services, to ensure that these products are secure by design and by default.

The widespread use of connected products in our daily lives without sufficient cybersecurity protection has made users increasingly exposed and vulnerable to serious cybersecurity risks. However, the increased risks for users have not been followed by a substantial improvement of the security functionalities incorporated in the design of connected devices.

Since 2016, BEUC members have conducted surveys on the growing use of connected devices at home, repeatedly demonstrating that too many connected products sold on the EU market come with **multiple cybersecurity risks and lack the most basic security features.**[2] A 2019 opinion from the European Union Agency for Cybersecurity (ENISA) Advisory Group reached a similar conclusion.[3] These products are putting consumers at risk on a daily basis.

Over the last years, **European consumers have become growingly aware and concerned** about the security of their products: a 2020 survey by the European Commission showed that **76% of consumers** believed that there is **an increasing risk of falling victim to a cybercrime**, while **78% avoided disclosing personal information online** because of cybersecurity-related issues.[4]

The CRA proposal is a welcome and necessary answer to a longstanding and repeated call for action from consumer organisations. However, it still **requires substantial improvements to fully address consumers' core concerns and expectations**.

This paper addresses the identified shortcomings and suggests key improvements to ensure that the CRA delivers a high level of cybersecurity and consumer protection.

2. A broader scope with very limited exclusions (Article 2)

BEUC welcomes that the CRA proposal sets a broad scope aiming to cover all connected products. According to **Article 2**, the CRA stands to apply to "products with digital elements whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network".

[1] 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, available at: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

[2] See below in Section 3, the outcomes of testing and surveys conducted by BEUC members across Europe on the cybersecurity vulnerabilities of connected devices.

[3] https://www.enisa.europa.eu/about-enisa/structure-organization/advisory-group/ag-publications/final-opinion-enisa-ag-consumer-iot-perspective-09.2019

[4] European Commission, Special Eurobarometer 499, Europeans' attitudes towards cyber security, January 2020: https://webgate.ec.europa.eu/ebsm/api/public/deliverable/download?doc=true&deliverableId=71905.

For the application of the CRA to be effective, **any exclusions to the scope must remain strictly limited and adequately justified**, thus ensuring that the CRA obligations apply to all relevant connected products which still remain without an adequate level of cybersecurity.[5]

However, the **scope of the CRA should be broadened further. It should clearly cover** not only all digital products and their ancillary services, including tangible digital products (wireless and wired hardware) and intangible digital products (embedded and non-embedded software), but also **web-based and cloud-based digital services** (such as Software-as-a-Service[6], online websites) available to consumers. This would allow to go further than the protection currently offered by the reviewed NIS2 Directive.[7] While web-based services already fall under the scope of the General Data Protection Regulation (GDPR, Articles 32-34, related to security of personal data processing), the **CRA goes beyond** the protection of personal data and provides a concrete **set of essential mandatory cybersecurity requirements**, such as **encryption** or **stronger authentication mechanisms** (e.g. two-factor authentication).

In 2022, BEUC's German member vzbv conducted a survey covering a total of 16 industry sectors, to determine **how often their digital services offered users an option to choose two-factor authentication solutions** and whether these solutions were optional, pre-set, or mandatory. After examining over 200 different digital services, checking the types of two-factor authentication offered and how secure they were, vzbv found that only a few and already regulated industry-specific areas offered comprehensive options for two-factor authentication.[8]

All digital cloud services should be clearly included within the scope of the CRA. These services are increasingly important to our economy and society. Following the Covid-19 pandemic,[9] there was a massive increase of demand for this kind of services across the board. These services have also become increasingly popular and important for consumers, who rely on them for multiple purposes, from the common use of cloud data storage (e.g. for smartphone photos), to device-syncing, both for personal and professional use.

BEUC recommendations

- **A broader scope covering all types of connected products** marketed to/intended for consumers and their associated services.

- The scope should be **expanded to cover all web-based services** (e.g. Software-as-a-Service, websites) available to consumers.

- All **digital cloud services** should be clearly included within the scope of the CRA proposal.

---

[5] Article 2(2) excludes products with digital elements within the scope of Regulation (EU) 2017/745 (medical devices for human use), Regulation (EU) 2017/746 (in vitro diagnostic medical devices for human use), as both Regulations contain requirements regarding devices, including on software and general obligations on manufacturers, covering the whole life cycle of products, as well as conformity assessment procedures. Products with digital elements certified under Regulation 2018/1139 (high uniform level of civil aviation safety), and Regulation (EU) 2019/2144 (type-approval requirements for motor vehicles) are also excluded.

[6] A Council non-paper on the principles of the CRA, issued by the representatives of Denmark, Germany and the Netherlands, has indeed called for this enlargement of the scope of the proposal: https://open.overheid.nl/repository/ronl-4865b2e8a7f5e4c48858fe5ad5bcb34aba70f645/1/pdf/joint-non-paper-cyber-resilience-act.pdf

[7] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555

[8] https://www.vzbv.de/pressemitteilungen/anbieter-und-hersteller-zu-it-sicherheit-verpflichten

[9] https://www.marketwatch.com/press-release/global-consumer-cloud-storage-services-market-expected-to-grow-usd-32902-million-business-statistics-development-data-forecast-period-2022-2028-2022-04-14

3. Mandatory and effective application of cybersecurity requirements

Consumer trust in the digital environment relies on the assumption that the products they acquire are both secure and safe to use. BEUC welcomes that the CRA will finally introduce **mandatory essential cybersecurity requirements for connected products,** enshrining the principle that all connected products should include, from their inception, cybersecurity functionalities according to their potential risks ('security by design'), and that their default settings should always be the most secure ones ('security by default').

The essential cybersecurity requirements detailed in Annex I establish not only the **properties of products** before being placed on the market (**Section 1**), but also the subsequent **handling of vulnerabilities** (**Section 2**).

The implementation of such security requirements by design and by default, covering key aspects such as **stronger authentication mechanisms, mandatory encryption, data minimisation** and the obligation to provide **security updates** are welcome developments. They will help tackle many of the security risks inherent to the nature of connected products[10] and limit some of the most negative potential consequences for consumers.[11]

3.1. Products should remain secure throughout their entire expected lifespan

Consumers have the right to expect that the products they acquire are fully developed and secure. When put on the market, connected devices should not only be **devoid of any known vulnerabilities, but also allow for key software updates** to keep devices secure and fit for purpose **throughout their lifetime**.

The CRA proposal rightly includes mandatory requirements on the handling of cybersecurity vulnerabilities. This effectively makes manufacturers **responsible for the 'continuous conformity'** of the products they place on the market, requiring them to **monitor and address vulnerabilities, and provide software updates**.

However, the proposal **still falls short of adequately protecting consumers** and their legitimate expectations regarding the **length of the period** during which this support is to be provided.

According to **Article 10(6),** manufacturers shall only have the obligation to ensure that vulnerabilities of their products are handled effectively and in accordance with the essential cybersecurity requirements "**for the expected product lifetime or for a period of five years** from the placing of the product on the market, **whichever is shorter**".

This obligation for 'continuous conformity' is therefore capped at a **maximum limit of five years, regardless of the actual lifespan of the products.** This arbitrary limitation period fails to consider the specificities of the usage and expected lifespans of all the types of connected products which this regulation is designed to cover.

This issue is **critical for consumers,** who have legitimate expectations that their products are **secure during a minimum period of time** corresponding to the **expected lifespan of the product** and its associated services. A recent survey[12] shows that **consumers already have an expectation** to receive security updates **for a much longer period** than what most manufacturers are willing to provide. Indeed, most respondents said that they **expect their devices** (in this case, smartphones, computers, smart TVs and gaming

[10] For example, the #ToyFail campaign by Forbrukerrådet, the Norwegian Consumer Council: the protection of the Bluetooth connection of the Cayla doll through strong authentication mechanisms, such as a unique password, could have prevented unauthorised access.
[11] https://www.which.co.uk/news/article/data-breaches-how-your-personal-details-end-up-in-the-hands-of-criminals-aWs6A1p3VSOJ
[12] https://privacyinternational.org/report/4965/we-looked-software-support-practices-5-most-popular-smart-devices-and-results-may#findings

consoles) to receive security updates for a period **between 2 to 10 years**, with many consumers already expecting these same products to receive updates for **even longer than 10 years**.[13]

Furthermore, recent examples from the industry demonstrate that **is perfectly possible for manufacturers to already offer guaranteed support for their products for longer periods,** apparently without significantly hindering their ability to innovate or doing business. Recent research carried out by BEUC member and UK consumer group Which? shows **that certain manufacturers of smart home appliances are already providing support for longer periods of time** which reflect the **minimum expected lifespan** of their products.[14]

This **obligation of 'continuous conformity'** under the CRA proposal **should therefore be in line with consumers' expectations**, be it for example two to three years for an electric toothbrush[15], 15 years for a smart refrigerator[16], 30 years for a smart television[17], or even longer in the case of operating systems which prove to be instrumentally resilient.[18]

The example of **Windows XP**[19] **shows just how such product lifespans can be underestimated.** Despite reaching the end of support in 2014, this operating system is still widely used globally by both consumers and public entities.[20] And it is not just a matter of updates. **Even XP's successors have their days numbered, literally**: Windows 8.1 support will end on 10 January 2023[21] and Windows 10 is only expected to be supported until 14 October 2025[22] (this despite Windows 11 having only made it onto 3% of consumer PCs[23]). Contrary to what the industry suggests, **neither can all products be upgraded** to newer versions (e.g. older hardware is often not equipped or able to upgrade to a new operating system), **nor can consumers simply ditch their products and buy new ones**, especially those consumers who are most vulnerable.

At the very least, the CRA proposal must therefore ensure that manufacturers of digital products are responsible for ensuring that the software of their products is **adequately and regularly updated** with vital system updates **throughout the expected lifespan of their products, and not limited to a period of only five years.**

A **period of five years** could eventually be a minimum, but **never a maximum threshold**. Software updates, **in particular security updates**, must be made available in a **timely manner for the whole duration of the expected lifespan of the product.**

[13] https://privacyinternational.org/press-release/4964/privacy-international-research-shows-smart-device-security-updates-fail-meet
[14] https://press.which.co.uk/whichpressreleases/smart-tvs-and-washing-machines-may-be-abandoned-by-brands-after-two-years-which-finds/
[15] http://www.designlife-cycle.com/electric-toothbush
[16] https://www.lifewire.com/smart-refrigerator-4158327
[17] http://www.koreatimes.co.kr/www/news/tech/2016/06/133_206377.html
[18] https://www.bleepingcomputer.com/news/microsoft/its-windows-xps-20th-birthday-and-way-too-many-still-use-it/
[19] https://support.microsoft.com/en-us/windows/windows-xp-support-has-ended-47b944b8-f4d3-82f2-9acc-21c79ee6ef5e
[20] https://www.bleepingcomputer.com/news/microsoft/its-windows-xps-20th-birthday-and-way-too-many-still-use-it/
[21] https://support.microsoft.com/en-us/windows/windows-8-1-support-will-end-on-january-10-2023-3cfd4cde-f611-496a-8057-923fba401e93
[22] https://www.cnet.com/tech/computing/windows-10-support-ends-in-4-years-but-this-is-what-you-should-know-now/
[23] https://www.forbes.com/sites/barrycollins/2022/10/10/windows-11-hits-only-3-of-pcs-in-first-year/

3.2. Risks of premature obsolescence and sustainability concerns on electronic waste

The introduction of an arbitrary **limit of five years** for software updates goes beyond cybersecurity and data protection concerns.[24] It would also raise significant issues regarding the **artificial limitation of the lifetimes of products at a time of growing sustainability and ecological concerns**.

The **lifespan of a product should not be artificially or arbitrarily limited** by the manufacturers but should be in line with the **realistic expectations of consumers**.

However, manufacturers have already been found to be either **refusing to provide security and functionality updates for longer periods** or even **pushing updates that reduce the functionality** of the devices.[25] Software updates can also be used by the manufacturers of a product to block or restrict independent repairs.[26] Such actions could potentially amount to **deliberate efforts** to push consumers to **discard their products** and replace them for newer ones[27] – a phenomenon which is known as '**premature obsolescence'**.[28]

BEUC member and UK consumer group Which? has consistently 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**[29] – even though 'smart' connected devices are by far more expensive and **have a greater life expectancy**.[30]

More importantly, the five-year limitation in the CRA proposal **goes against the current market[31] and legislative trends** (e.g. proposals on Right to Repair[32], Ecodesign for Sustainable Products Regulation[33]), which have been proposed to incentivise businesses to **become and act more sustainable** and **produce longer lasting products** to address the growing environmental and sustainability risks, in particular the increase of electronic waste. Such a limitation therefore **appears counterproductive and would convey the wrong message** at a critical time when trends for more sustainable and ecological product design are taking off.

For example, the proposed Commission Regulation laying down **Ecodesign requirements for mobile phones, cordless phones and tablets**[34] states that software security updates

[24] For additional insight on BEUC position on IoT and connected devices, please see our position paper: https://www.beuc.eu/publications/beuc-x-2021-091_protecting_european_consumers_in_the_world_of_connected_devices.pdf

[25] https://www.howtogeek.com/731791/what-is-planned-obsolescence-and-how-does-it-affect-my-devices/

[26] https://repair.eu/news/part-pairing-a-major-threat-to-independent-repair/

[27] In December 2020, Test-Achats and OCU, BEUC's Belgian and Spanish members respectively, launched class action lawsuits against Apple over the planned obsolescence of the Apple iPhone. See https://www.test-achats.be/actions-collectives/apple-iphone

[28] See BEUC Position Paper on "Durable and Repairable Products: Changes needed for a successful path towards the green transition": https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-061_durable_and_repairable_products_beuc_position_paper.pdf

[29] https://press.which.co.uk/whichpressreleases/smart-tvs-and-washing-machines-may-be-abandoned-by-brands-after-two-years-which-finds/

[30] https://press.which.co.uk/whichpressreleases/a-fridge-too-far-the-smart-appliances-that-cost-a-grand-more-but-may-only-last-two-years/

[31] https://www.forbes.com/sites/sap/2022/02/15/sustainability-trends-2022-a-make-or-break-moment-for-consumer-product-supply-chains/

[32] Upcoming European Commission proposal for a directive on the Sustainable consumption of goods – promoting repair and reuse: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13150-Sustainable-consumption-of-goods-promoting-repair-and-reuse_en

[33] Proposal for Ecodesign for Sustainable Products Regulation, part of the European Commission's approach to foster more environmentally sustainable and circular products: https://ec.europa.eu/info/energy-climate-change-environment/standards-tools-and-labels/products-labelling-rules-and-requirements/sustainable-products/ecodesign-sustainable-products_en

[34] Proposed Commission Regulation laying down Ecodesign requirements for mobile phones, cordless phones and slate tablets pursuant to Directive 2009/125/EC: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELLAR:955d36e7-2906-11ed-8fa0-01aa75ed71a1

for these products must be provided for a **minimum of five years**. The CRA proposal should be coherent with this legislation. The **period of five years** from the placing of the product on the market could therefore be considered as a minimum threshold of protection, but **not as a limiting cap preventing support during the expected lifespan of the product**.

3.3. Software updates: unbundling security and functionality updates

Consumers have a reasonable expectation that the products that they acquire will be continuously updated by their manufacturers to ensure the highest levels of security and functionality. However, manufacturers do not always make clear what these software updates contain or for what purpose they are necessary. **Consumers are left in the dark** as to whether their latest software updates are to improve cybersecurity of their devices, install new OS functionalities or even install other 'hidden' features which may have undesired or negative effects on their devices.

There are ample **reports of consumers struggling with unexpected effects** on their connected products after installing certain software updates.[35] For instance, in November 2020, the Italian Competition Authority (AGCM) found that Hewlett-Packard (HP) **misled consumers who acquired its printers** since 2016, by encouraging updates to new firmware while **omitting its actual impact** on the use of non-original ink/tone cartridges, which prevented consumers from using third party cartridges.

The CRA proposal **should bring more transparency and differentiation regarding software updates**. The proposal **should oblige manufacturers to differentiate between security updates** (to provide devices with enhanced security, including security patches) and **corrective or functionality updates** (to provide corrective or new functionalities, including corrective patches), establishing that these updates **should be provided separately**, unless clearly demonstrated that it is not technically possible.

Manufacturers **should always have to clearly explain the reason behind each update** as well as its **foreseen impact** on the product.[36] While security updates must be installed immediately and automatically, this should not be the case with functionality updates: users should **be informed ahead of the installation** about the potential impacts of the functionality updates in order to **effectively review their contents and make an informed decision on whether to accept or reject** their installation. More importantly, the refusal of functionality updates must not impact the security and protection of the product.

In 2018, following reports by BEUC's Italian member Altroconsumo,[37] the Italian Competition Authority (AGCM) found that Samsung and Apple had engaged in unfair commercial practices, by **pushing software updates which significantly reduced the performance and functionality of their mobile phones**: the firmware updates "caused serious malfunctions and significantly reduced their performance, in this way speeding up

[35] In May 2022, BEUC Italian member Altroconsumo conducted a survey on rise of connected smart devices at home: one third of respondents experienced functioning problems with smart devices, with 30% of those stating to have encountered malfunctions immediately after installing software updates: https://www.altroconsumo.it/organizzazione/media-e-press/comunicati/2022/internet-delle-cose

[36] In November 2020, the Italian Antitrust Authority found that HP, since (at least) the end of 2016, misled consumers, encouraging updates to new firmware while omitting its impact on the use of non-original ink/toner cartridges, in order to falsely persuade consumers not to use third party cartridges. Recently, Test-Achats, OCU, DECO Proteste and Altroconsumo, our Belgian, Spanish, Portuguese and Italian members respectively, reached a settlement agreement with HP after asking the company to pay damages to consumers: https://www.euroconsumers.org/activities/hp-and-euroconsumers-reach-a-settlement-on-dynamic-security-dispute.

[37] https://www.altroconsumo.it/organizzazione/media-e-press/comunicati/2018/obsolescenza-programmata-oggi-con-antitrust-i-frutti-della-battaglia-iniziata-nel-2014

their replacement with more recent products".[38] Collective action against such practices harming consumers is currently ongoing.[39]

French authorities followed up more recently in 2020, imposing new penalties on Apple[40] for "deceptive commercial practice by omission" when **failing to inform consumers** that installing iOS updates (10.2.1 and 11.2) could slow down older devices. Apple confirmed in 2017 that it deliberately slowed down older iPhone models, arguing that a device performance management was necessary due to lithium-ion batteries being less capable of supplying peak current demands over time. [41]

This type of information **should be provided to the consumer, who should make the decision, rather than be denied by default**. [42]

BEUC recommendations

- Manufacturers should be obliged to monitor and address security vulnerabilities in accordance with the essential cybersecurity requirements **during the entire expected lifespan of a product**, and **not be limited** to a maximum period of **five years.**

- A threshold of five years from the placing of the product on the market could act as a minimum threshold, **but not as a limiting cap** preventing support during the expected lifespan of the product.

- **Software updates must be unbundled**: security and functionality updates must be considered as **separate types of updates** and be **provided separately**.

4. Strengthening the conformity assessment procedure

4.1. Self-assessment by default means cybersecurity at risk by design

The proposed overall conformity assessment procedure **should be strengthened**. Although the CRA sets essential cybersecurity requirements for mandatory compliance in Annex I, the Commission proposal **relies excessively on self-assessment**. The Commission's own estimates show that **over 90% of products** covered by this proposal would be **subject to self-assessment**.[43] Leaving it to the corresponding industry to carry out its own unvetted assessment of compliance with essential cybersecurity requirements is a **flawed solution** which will **undermine consumer trust** and **compromise the effective application of the CRA.**

First, there are **clear conflict of interests** when those responsible for assessing compliance with the CRA requirements are the exact same companies which are subject to those legal requirements, and which are eager to place their products on the market as quickly as possible.

Cybersecurity risks are often ignored by manufacturers, as their main objective is to place their product on the market as fast as possible ('short time to market'). There is consistent and sufficient evidence of market pressures leading manufacturers to either

[38] AGCM imposed penalties on Samsung and Apple of 5 million Euros and 10 million Euros, respectively: https://en.agcm.it/en/media/press-releases/2018/10/PS11009-PS11039
[39] BEUC Belgian member Test-Achats has brought a collective action against Apple for premature obsolescence of model iPhone 6: https://www.test-achats.be/actions-collectives/apple-iphone
[40] https://www.economie.gouv.fr/dgccrf/transaction-avec-le-groupe-apple-pour-pratique-commerciale-trompeuse
[41] https://www.bbc.com/news/technology-42438745
[42] https://www.bbc.com/news/technology-51413724
[43] https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-impact-assessment

underestimate the impact of product vulnerabilities[44] or fail to adopt transparent practices for vulnerability disclosure.[45]

There are also significant **shortcomings in companies' cybersecurity resources and expertise** to consider. Many manufacturers and distributors of products of lower technical complexity **may not have the necessary skillset** to guarantee an adequate level of cybersecurity to begin with, often failing to account for possible cybersecurity vulnerabilities issues when manufacturing, importing or reselling connected products.

In addition, there are concerns that the excessive reliance on self-assessment for the large majority of products **could roll back the existing protection** under the Radio Equipment Directive (RED)[46], and its Delegated Act[47], therefore actually **lowering – instead of raising – the level of cybersecurity protection**.

Representatives of certification bodies have warned that self-assessment under the CRA proposal would effectively **"water-down" the levels of protection of the RED Directive** and its Delegated Act, which "allows for self-assessment (Module A) only if harmonised standards have been fully applied, [while] the CRA allows a self-assessment for "baseline" products in any case regardless of whether harmonised standards have been fully applied or not."[48] Moreover, the RED Directive requires an **independent assessment by notified bodies** when product manufacturers have not fully applied the harmonised standards that specify the essential cybersecurity requirements.

The establishment of a new horizonal regulation on mandatory cybersecurity requirements is a unique opportunity to **increase the levels of protection for consumers**. The CRA proposal **must not allow any potential loopholes which risk watering down or rolling back existing levels of protection.**

Additionally, the CRA should better **explore the interplay between safety and security**. Many products already undergo a mandatory third-party assessment of their safety features as a result of EU sectoral legislation. For all these products, the evaluator should check whether a security breach could have an impact on the safety features of the product. Should this be the case, a **cybersecurity assessment**, in line with the CRA requirements, should be mandatory as part of the overall conformity assessment procedure.

4.2. Presumption of conformity, self-assessment through the 'backdoor'?

Article 18 of the CRA proposal establishes a **presumption of conformity** for products with digital elements and processes: these products and processes are presumed to be in conformity with the essential requirements of the CRA if the manufacturer has followed **harmonised standards, common specifications or a European cybersecurity certification scheme**.

This **establishes a problematic equivalence between different instruments** which are not comparable in their scope of protection. **European cybersecurity certification**

[44] In 2022, the German Federal Office for Information Security (BSI) issued a warning over a faulty digital door lock. A critical vulnerability was detected in the product „HomeTec Pro CFA3000" manufacturered by ABUS, which allows nearby attackers to lock and unlock the radio signal door lock in order to gain access to buildings, offices or apartments https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Warnungen-nach-P7_BSIG/2022/BSI_W-005-220810.pdf?__blob=publicationFile&v=12

[45] https://www.theverge.com/2022/10/16/23405739/microsoft-out-of-date-driver-list-windows-pcs-malware-attacks-years-byovd

[46] Directive 2014/53/EU on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0053

[47] Commission Delegated Regulation (EU) 2022/30, of 29 October 2021 supplementing Directive 2014/53/EU with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f): https://eur-lex.europa.eu/eli/reg_del/2022/30/oj

[48] TÜV Verband Position Paper on the Commission proposal for a Cyber Resilience Act: https://www.tuev-verband.de/?tx_epxelo_file[id]=905395&cHash=d311b8d964793f7d5d56f74fc1c25036

schemes are established by EU legislation under the Cybersecurity Act (CSA)[49], where certification relies on the **assessment of an independent third party**, with **self-assessment only considered** for "basic" certification level, i.e. for products of "low complexity" that present "**a low risk to the public**."[50]

More particularly, the European cybersecurity **certification level "high"** corresponds to the **highest level of assurance** provided by the CSA. A product that is certified "high" level is evaluated at a level intended to **minimise the risk** of state-of-the-art cyberattacks carried out by actors with significant skills and resources.[51] **Harmonised standards** and ad hoc **common specifications would fail to meet** that threshold.[52]

European testing, inspection and certification organisations have already expressed their **fears that the CRA proposal may become a "toothless tiger"**[53], should the proposal fail to establish **more effective instruments to assess compliance.** Placing such instruments on an equal footing would **provide encouragement** for economic operators to **rely almost exclusively on harmonised technical standards** and avoid third-party assessment to clearly ensure that the newly introduced **cybersecurity requirements are reliably verified.**

At the very least, third-party assessment should be the rule to assess the conformity of **products of higher cybersecurity risk**. 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**. Failing to clarify this aspect could amount to **self-assessment through the 'backdoor'**, contributing to further undermine the application of the essential requirements laid out in the CRA proposal.

4.3. The Role of Standards in ensuring cybersecurity for consumers*

The presumption of conformity for products with digital elements and processes established under **Article 18** of the CRA proposal **would rely on the development and application of harmonised (technical) standards by** the European Standardisation Organisations and manufacturers, respectively.

This provision, based on the New Legislative framework and similar to the approach taken in the Artificial Intelligence Act[54] proposal, implies a **reversal of the burden of proof** regarding the compliance with the essential requirements set out in Annex I. The public authorities in charge of market surveillance will have the burden to prove lack of compliance. **This is a point of concern** when it comes to the conformity assessment of critical products considered of higher risk. **Under Article 24(2)** of the CRA proposal, manufacturers of critical products listed under Class I of Annex III who have **applied harmonised technical standards** would be allowed to carry out a **conformity self-assessment**.

Technical standards are a useful part of a wider regulatory and governance context for cybersecurity. Technical standards can deliver the technical robustness, security and interoperability required to meet some elements of consumer expectations and needs. However, the **excessive reliance on harmonised technical standards and self-assessment** procedure by the CRA to ensure that essential cybersecurity requirements

[49] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act
[50] Cybersecurity Act, Recital 79.
[51] Cybersecurity Act, Article 52 (7).
[52] https://www.tic-council.org/application/files/9515/8694/5697/2018_Feb_13_Revised_-_Selecting_Methods_of_Conformity_for_Regulatory_Schemes.pdf
[53] https://www.tuev-verband.de/en/news-release/tuev-association-calls-for-further-tightening-of-the-cyber-resilience-act
** This section is co-authored by BEUC and ANEC - https://www.anec.eu/*
[54] See BEUC and ANEC comments on the use of harmonised standards in BEUC Position Paper on the AI Act https://www.beuc.eu/sites/default/files/publications/beuc-x-2021/088_regulating_ai_to_protect_the_consumer.pdf

are applied by manufacturers **raises serious issues from a consumer protection** standpoint and ultimately fails to address the legitimate concerns of consumers.[55]

Firstly, the use of **harmonised technical standards cannot be a replacement for legislation**. Technical standards should function as "technical specifications for repeated or continuous application" (as defined in Article 2(1) of Regulation 1025/2012 on European Standardisation). Therefore, technical standards should only be used to define technical requirements, and **not to define or interpret legal obligations**.

For instance, a technical **standard should not be used as a basis for presuming conformity in Article 24(2)** for assessment of the conformity of 'critical products with digital elements' listed under Class I, Annex III. The submission of critical products listed under Class I to *de facto* self-assessment via the assurances by manufacturers that they have applied harmonised technical standards stands to **significantly compromise the effectiveness of the application** of the legal cybersecurity requirements introduced by the CRA proposal in Annex I and consequently undermine the principle of cybersecurity by default and by design. We therefore believe that, **at the very least, third party assessment should be used for all critical products.**

Secondly, there is **limited participation of civil society and consumer organisations** at national, European and international **standardisation bodies**, which are essentially driven by industry. The influence of consumer organisations in these bodies is limited, due to a lack of resources and expertise at national level, as well as the setup of their decision-making processes, which are based on the national delegation principle.

Moreover, the **increasing push of the industry**, reflected by the National Standardisation Bodies who sit in the European Standardisation Organisations, **to set a single, globally relevant standard is encouraging a convergence** between European and international standards. From a European perspective, given the primacy of international standardisation over the regional, the consequence would be that more standards for application within Europe are being drafted or revised at the international level. The **participation of consumers and civil society is even more limited in international standardisation discussions**, while there is a strong participation of countries that do not share European values and principles, especially in AI standardisation.

The **adoption at European level of several international standards** on organisational frameworks and methodologies (e.g. IT management systems; data protection and privacy guidelines; processes and products evaluation schemes; ICT security and physical security technical guidelines) is **already taking place.** While the availability of such international standards might help in raising the level of security across the world, and their adoption as European standards will ensure they are transposed into national standards catalogues throughout the Single Market, we do not see these standards as containing sufficient security requirements which can increase consumer trust in the connected products they buy. We therefore call for caution and scrutiny **whenever international standards are used to implement European public policies and legislation**, especially in the context of cyber resilience against geopolitically motivated attacks. We suggest that the European Commission should be able to adopt common specifications not only in the absence of standards, but also to protect consumers in case their fundamental rights are at risk.

In conclusion, the CRA establishes clear and detailed cybersecurity requirements which should be observed by manufacturers of digital products. Critical **products which can be considered of higher risk should therefore have their conformity assessed exclusively by third parties** on the basis of such legal requirements.

[55] Several academics and organisations have explained in detail how the use of standardisation can undermine the EU's democratic process. See Michael Veale, Frederik Zuiderveen Borgesius (no 8); Martin Ebers, Standardizing AI – The Case of the European Commission's proposal for an Artificial Intelligence Act, in: Larry A. DiMatteo/Michel Cannarsa/Cristina Poncibò (eds.), The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics, pending for publication, 22 pages, Cambridge University Press 2022.

BEUC and ANEC recommendations:

- The **conformity assessment procedure should be strengthened** in order to avoid overdependence on self-assessment.

- **Harmonised technical standards must not be used** to define or apply legal obligations and requirements, and should be limited to implement technical aspects.

- **Third party assessment should be applied to all 'critical products with digital elements'**, independently from the use of technical standards. The use of technical standards for conformity self-assessment under Article 24(2) of 'critical products' (Class I, Annex III) **must be avoided**.

- The **governance system of the standardisation process must be changed significantly**. Consumer organisations must be systematically involved in standardisation. The European Commission's standardisation strategy must quickly be implemented to improve the situation in this regard.

- Public authorities must also provide political and financial frameworks that allow for the **participation of all stakeholders, including consumers** and broader societal interests

- Given that public authorities have also withdrawn from many standardisation activities to the detriment of the public interest, we call on **authorities to become more engaged in standardisation** and **support consumer participation** in it.

5. Mandatory third-party assessment for critical products, including consumer products (Annex III)

5.1. The absence of a risk assessment methodology

We welcome that the application of essential cybersecurity requirements is complemented with mandatory cybersecurity certification for products considered of higher risk, as BEUC requested. However, we regret that the proposal ultimately misses the opportunity to put forward an **objective risk assessment methodology and a clearer definition of risks**.

Ultimately, the choice for the CRA proposal was to adopt a **'closed-list approach'**, by identifying specific categories of 'critical products' considered to be of higher cybersecurity risk in Annex III. The current list of products is itself divided into two classes: **Class I for 'critical products' of lower risk**, and **Class II**, for those considered of **higher risk.**

The criteria used to define the products which fall in each of the two categories is not clear and their future updates **disproportionately rely on implementing and delegated acts** by the European Commission, thus removing predictability and legal certainty from this key aspect of the proposal. This approach ultimately seems **ill-adapted to make the CRA a law which is well-suited to future developments** in products and the market.

We therefore propose that the CRA proposal should **establish clear legislative criteria** to determine which products should be considered critical products of higher risk. These criteria should include, for instance, the **sensitivity of the data processed by these products**, the **risks entailed by their normal use**, but also the **potential dangers** that these devices may represent in case of a successful cyberattack, **including potential physical harm** for consumers.

The **definition of cybersecurity risk must be broader and more comprehensive**. Besides the protection of the physical integrity, a risk assessment must always consider

potential threats to fundamental rights and the safety or integrity of an individual. It must also include a risk matrix where probability and consequence are considered to set out mitigation measures, together with a list of categories of personal data processed by the device in question.

In the case of **consumer products**, they should clearly be considered critical products of higher risk, when either their **intended use or reasonably foreseen misuse** caused by a cyberattack **creates a risk of harm to their health and safety, or a risk of adverse impact on fundamental rights** (including privacy and data protection) of the users.[56]

5.2. The necessity of mandatory certification for all 'critical products'

The safest way to ensure consumers are adequately protected is, **at the very least, to require that products considered to represent a higher risk of cybersecurity undergo a third-party assessment**.

The most effective way to achieve that would be for the CRA proposal to require all 'critical products with digital elements' listed in Annex III to undergo **mandatory European cybersecurity certification at the level of assurance set at "high" as established in the Cybersecurity Act (CSA**).[57] This requirement should cover **both Class I and Class II** products.

The justification for this measure is that a successful cyber-attack against these products **could have terrible, harmful consequences for consumers**. It is important to look at the type of data at stake to understand the sensitivity of these products. In the case of password managers (Class I), a successful cyber-attack could mean that users would see all their accounts compromised, leading to grave economic harm (e.g., bank credentials stolen) or social prejudice.

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.[58] This incident showed that **security at state-of-the-art level is a prerequisite for such products**. The assets at stake are simply **too valuable and will inevitably attract well-trained cyber-offenders**.

The same could be said for the other products listed in both Class I and Class II of Annex III. An attack on internet routers could compromise the integrity of a consumer's private network, while an attack on a secure element could lead to a cyber-attacker having access to the most sensitive cryptographic operations performed in a smartphone (e.g. PIN code, authentication etc).

The CRA proposal should therefore explicitly refer to the CSA level of assurance "high", when referring European cybersecurity certification for 'critical products'. **Testing laboratories** should not only check that the security functionalities are correctly implemented but **should also try to hack the devices in question,** by using an evaluation method called **'penetration testing'. Only the European cybersecurity certification at the level "high" (CSA "high") ensures that penetration testing is performed on a product.** Other CSA levels ("basic" and "substantial") do not include penetration testing and, more generally, do not guarantee resistance against skilled attackers.

An additional reason to opt for a mandatory CSA certification is the **stringent process for the drafting and approval of European certification schemes**. ENISA drafts the

[56] Please see BEUC Position Paper on AI Act: https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-088_regulating_ai_to_protect_the_consumer.pdf
[57] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019R0881
[58] https://www.forbes.com/sites/daveywinder/2022/08/25/lastpass-hacked-password-manager-with-25-million-users-confirms-breach/?sh=3068fd637d5a .

candidate scheme, with the support of national cybersecurity agencies and selected stakeholders. This process greatly differs from the classical standardisation process, which tends to be more industry-driven. **In the case of certification schemes, public authorities are in the driving seat.**

At the moment, ENISA is still rolling out certification schemes, with the European Union Cybersecurity Certification (EUCC) scheme being ready and the European Union Cybersecurity Certification Scheme on Cloud Services (EUCS) scheme already well-advanced. Work on the 5G scheme has also started. Future schemes can rely on those previously adopted schemes, as building blocks. However, we call on the European Commission to analyse whether existing certification schemes cover the entire list of products in Annex III. **If the European Commission identifies gaps, we suggest sending requests to ENISA as early possible to prepare the missing certification schemes.**

5.3. List of 'critical products' must be extended beyond mere industrial use

The list of 'critical products with digital elements' in Annex III has an **excessive focus on products of mere industrial use**. In the current text, the listing of critical products of higher risk in Class II includes products such as **internet routers or firewalls, yet only those "intended for industrial use".**

This is problematic, especially following the Covid-19 pandemic, where teleworking has effectively blurred the lines between personal and professional use, exposing companies to cybersecurity vulnerabilities.[59]

The most evident case is **internet routers,** which are key for cybersecurity while **remaining one of the most insecure devices**. In the year of 2021 alone, 500 vulnerabilities were discovered in these devices, including 87 considered critical.[60] As the gateway to the Internet, **routers are essential** for Wi-Fi connections and act as a **hub for the entire home or office network**. It is through a router that all smart home devices can access the internet and exchange data. Should a router be compromised by a cyberattack, hackers can gain access to private and professional networks and obtain all kinds of private and personal data, possibly causing irreparable damage.[61]

Given the **extremely sensitive nature** of these products, the versatility of their use, as well as the singularity of the manufacturers and manufacturing lines that produce them, routers **should always require third-party assessment**.

At the very least, the scope of the listing in Annex III must **therefore be expanded and cover all "internet routers, modems** intended for the connection to the internet" as well as "**firewalls, intrusion detection** and/or prevention systems".

5.4. Consumer products must be added to the list of 'critical products'

BEUC regrets that **connected devices used by consumers are mostly absent** from the list of 'critical products with digital elements' of higher risk under Class II of Annex III, and therefore **not submitted to the obligation of a third-party assessment**.

At the very least, the list of 'critical products with digital elements' with mandatory third-party assessment **must be expanded to recognise the necessity for independent third-party assessment of certain consumer products** that pose higher risks to consumers.

[59] https://www.cybernewsgroup.co.uk/discovered-vulnerabilities-in-d-link-router-causes-serious-worries-about-remote-worker-it-security/
[60] https://www.kaspersky.com/about/press-releases/2022_87-critical-vulnerabilities-discovered-in-routers-in-2021
[61] https://securelist.com/router-security-2021/106711/

Annex III should include in its Class II list the following categories of products:

- **Private security devices** e.g. smart security alarms, smart smoke detectors or carbon monoxide alarms, digital door locks, security cameras and private surveillance equipment.
- **Smart home devices** e.g. electricity control, heating or cooling appliances or ventilation in smart homes.
- **Connected toys and other devices intended to interact with children** e.g. toys relying on active connection to function, baby monitors, educational devices and wearables for children.
- **Health appliances and wearables** e.g. fitness trackers, smart watches, panic buttons, wearables for minors.

5.4.1. Private security devices

Consumers have reasonable expectations that connected products designed to make them safe should be themselves especially secure. However, the fact remains that **security devices are renowned for their critical cybersecurity vulnerabilities.**[62]

Moreover, security devices particularly stand out as an example of consumer devices where **vulnerabilities should be considered as critical products of high risk**, as the hacking of security and alarm systems can reasonably be **expected to be driven by a criminal intent**.[63]

Indeed, one of the most trending vulnerabilities is the **proliferation of spying software** designed to track the activity of users across their devices:[64] "spyware" allows hackers to take control of consumers' surrounding environment, by hacking their devices in order to access their private data and track their activity.

A particularly invasive type of spying software is '**stalkerware'**, which allows malicious actors to **target the devices of a specific individual** to invade their privacy by monitoring their daily activities. Online stalkers can therefore take advantage of connected products with embedded microphones and cameras in the immediate surroundings of their target to **access their most private moments without consent**. [65]

BEUC members have **consistently exposed how such critical vulnerabilities in security devices can be easily exploited**. In 2017, BEUC member Which? from the United Kingdom 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.[66]

This was followed in 2018 by BEUC's Belgian member Test-Achats (TA) who launched the "Hackable Home" campaign. Having equipped a home with a broad range of smart devices, TA gave ethical hackers a week to take control of some products. Out of 19 connected appliances (a smart fridge, thermostat, security cameras, door locks, loudspeaker, robot vacuum cleaner), **half of the products 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**.

---

[62] https://www.bleepingcomputer.com/news/security/new-hacking-tool-lets-users-access-a-bunch-of-dvrs-and-their-video-feeds/
[63] https://www.which.co.uk/news/article/more-than-100000-wireless-security-cameras-in-the-uk-at-risk-of-being-hacked-a0vVp2v8zNqx
[64] https://tcrn.ch/3p80HcR
[65] https://www.laptopmag.com/features/spyware-vs-stalkerware-whats-the-difference
[66] https://press.which.co.uk/whichpressreleases/the-hackable-home-investigation-exposes-vulnerability-of-smart-home-devices/

More recently in 2022, the German Federal Office for Information Security (BSI) warned about a **faulty digital door lock with a critical vulnerability** that allowed nearby attackers to lock and unlock the radio signal door lock in order to gain access to buildings, offices or apartments.[67]

5.4.2. Smart home devices

Smart home devices are especially critical, given their **functionalities** and their sensitive location inside our homes, **an environment which must be especially private and secure**. Smart home appliances connected to a broad network system may be used to **compromise the fundamental right to privacy as well as the personal data of users**. In 2022, for instance, smart vacuum cleaners were found to be collecting image and audio on their users as well as data on their homes' immediate surroundings.[68]

Moreover, these **systems may also be instrumentalised to compromise the health and safety** of those who live in the targeted house (e.g. hacking electricity control, heating systems of smart homes).[69] In 2021, BEUC's Belgian member Test-Achats (TA) repeated the **"Hackable Home" campaign** with a similar exercise: out of 16 home connected devices (smart televisions, smart vacuum cleaners, baby monitors, door locks and alarm systems), **ethical hackers found 54 different vulnerabilities**, with 10 connected devices showing a serious or critical vulnerability. These vulnerabilities mean these devices can be **easily accessed and controlled from a distance by malicious actors**.[70]

5.4.3. Connected toys and other devices intended to interact with children

Connected toys pose especially significant risks given their **unfettered access** to the inside of the family home and their **direct access to children**. Given the **growing use of built-in audio and video collection hardware**, the potential for surveillance monitoring and concerns for personal safety and physical integrity grow. Moreover, these specific cybersecurity vulnerabilities stand to have a long**-term impact on children**, should harm materialise.

In 2016, our Norwegian member and consumer group Forbrukerrådet, demonstrated how a connected toy could become a real-life illegal spying device[71] and a substantial risk to the safety of children. It was found that a **children's doll named Cayla could be easily hacked** in just a few simple steps. Attackers could connect from a distance and **directly speak to the children through the toy,** thus putting the children's physical safety and privacy at risk.[72]

More recent investigations by BEUC members[73] show how malicious hackers may exploit the cybersecurity vulnerabilities in different products intended to interact with children. For example, **connected playing dolls[74] and baby monitors[75] may have their inbuilt microphone, camera and speaker** used to communicate with **children** or to **spy on**

---

[67] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Warnungen-nach-P7_BSIG/2022/BSI_W-005-220810.pdf?__blob=publicationFile&v=12

[68] https://www.technologyreview.com/2022/12/19/1065306/roomba-irobot-robot-vacuums-artificial-intelligence-training-data-privacy/

[69] https://www.which.co.uk/news/article/how-the-smart-home-could-be-at-risk-from-hackers-akeR18s9eBHU

[70] https://www.test-achats.be/hightech/smart-home/presse/la-securite-des-appareils-domestiques-intelligents-est-une-veritable-passoire

[71] Following a Cold War era legislation, Germany's Federal Network Agency 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

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

[73] https://www.which.co.uk/news/article/popular-baby-monitor-app-put-privacy-at-risk-atCnH3W8bpgZ

[74] https://www.theguardian.com/world/2017/feb/17/german-parents-told-to-destroy-my-friend-cayla-doll-spy-on-children

[75] https://www.computerworld.com/article/2476196/hacker-strikes-again--creep-hijacks-baby-monitor-to-scream-at-infant-and-parents.html

parents.[76] Moreover, there is also a growing trend to use ordinary, often **unsafe online cameras** for the purpose of baby monitoring.[77]

In 2022, BEUC's Portuguese member, consumer group DECO, conducted a test on this category of products, **having found numerous flaws** with 17 connected products aimed at babies and children. Five devices had a critical vulnerability, seven others a vulnerability with a medium to high severity. DECO also found that unbranded products or those from less well-known brands registered more severe vulnerabilities than those products manufactured by more popular brands.[78]

Therefore, **connected toys** and products which interact with children must be **obliged to undergo third-party assessment**. Given that this is a very particular risk which concerns cyber security vulnerabilities, the CRA would be the most adequate legal instrument where to set this obligation, which at present is not covered by the Toy Safety Directive.

5.4.4. Health appliances and wearables

Cybersecurity vulnerabilities can have a long-term impact on the health and safety of product users. Compromised devices such as health appliances and wearable devices[79] with inbuilt audio or video hardware, health data monitoring or location software pose risks of surveillance monitoring, health safety or even blackmail.[80]

This is especially accurate in the case of the **most vulnerable consumers**. In 2017, BEUC member Forbrukerrådet tested the **security features of smart watches for children**[81] which enable parents to keep in touch and track their child's real-time location. **They discovered very serious security flaws**, including the possibility for an attacker to track and contact children directly or even alter the geo-location (location spoofing) of the watch.

Moreover, health appliances and wearables collect substantial amounts of data. **Health data in particular are highly sensitive data** (defined as sensitive under Article 9 GDPR). Their disclosure, loss or theft can have long-term consequences, and lead to potential threats and damage to consumers, not only in terms of their privacy but also regarding potential economic harm (reduced chances to obtain a job offer, more expensive insurance premiums etc). Therefore, such devices should require – and be independently assessed for - the highest level of data security.

BEUC recommendations

- **Mandatory CSA certification level "high" for all products listed in Annex III,** discarding other options, especially those relying **on self-assessment.**

- **Analyse the availability of CSA certification schemes for the certification of critical products (Annex III)**, identify potential missing schemes and, if necessary, send scheme requests to ENISA as soon as possible.

- **At the very least**, **enlarge the scope** of the list of 'critical products with digital elements' (Annex III, Classes I and II) **beyond products of mere industrial use**. For example, **all types of internet routers, firewalls, modems** must be included, regardless of their intended use.

[76] https://www.itsecuritynews.info/hackers-exploit-camera-vulnerabilities-to-spy-on-parents/
[77] https://www.which.co.uk/news/article/which-warns-parents-not-to-use-a-security-camera-as-a-baby-monitor-aRKrN2F0jF77
[78] https://www.deco.proteste.pt/tecnologia/telemoveis/noticias/aparelhos-ligados-net-partilham-dados-criancas
[79] https://www.democraticmedia.org/blog/health-wearable-devices-pose-new-consumer-and-privacy-risks
[80] For more information, see BEUC position paper on the proposal for a European Health Data Space (EHDS): https://www.beuc.eu/sites/default/files/publications/BEUC-X-2022-104_Position_paper_on_the_proposed_European_Health_Data_Space.pdf
[81] https://fil.forbrukerradet.no/wp-content/uploads/2017/10/watchout-rapport-october-2017.pdf

- **Consumer devices must also be added** to the list of 'critical products with digital elements' of higher risk (Annex III, Class II). In particular:

  - Private security devices.
  - Smart home devices.
  - Connected toys and other devices intended to interact with children.
  - Health appliances and wearables.

6. Stronger market surveillance and enforcement framework (Chapter V)

BEUC has consistently raised concerns regarding the lack of an effective enforcement framework in EU law allowing manufacturers and distributors of connected devices to be held accountable for their products' cybersecurity flaws.[82]

We therefore **welcome the introduction of a market surveillance and enforcement framework in Chapter V** of the CRA proposal, enabling **national authorities to conduct effective market surveillance and to enforce effective sanctions** against economic operators for non-compliance with the requirements set out in this legislation. We especially welcome that surveillance authorities should have the **power to withdraw products from the market** when they do not comply with cybersecurity requirements.

However, the proposed governance structure **rests mainly at Member State level** with national market surveillance authorities. This raises **concerns of possible shortcomings in terms of resources** and '**enforcement bottlenecks'**, similar to those experienced under the GDPR.[83]

In light of this, we **welcome that the proposal tries to address some of these shortcomings by giving a clear role to the European Commission.** Article 45 of the CRA proposal establishes a **"procedure at EU level** concerning products with digital elements **presenting a significant cybersecurity risk**". We strongly agree with empowering the **Commission, under Article 45(1), to proactively take the lead** and request that the relevant market surveillance authorities start an evaluation procedure whenever it has sufficient reasons to believe that a product with digital elements presents a significant cybersecurity risk and has failed to comply with the CRA obligations.

Moreover, we welcome that Article 45(2) especially foresees the **fall-back option** for the Commission to intervene and start an evaluation procedure **in case of inaction of the national market surveillance authority**. The safeguard mechanism as introduced with the **Union Safeguard Procedure** (Article 44) is also welcome.

However, we are concerned that the fall-back option as designed in Article 45 **may be too little, too late** – or not come at all, as the Commission reserves the right to exercise its powers and is **only obliged to intervene under Article 45(2) in "exceptional circumstances** which justify an **immediate intervention** to preserve the good functioning of the internal market" and where the Commission has "**sufficient reasons to consider** that the product remains non-compliant".

[82] Although the RED directive does include market surveillance mechanisms, the scope of the products covered by the RED is limited, not covering all connected devices. For example, while covering wireless connected products, it leaves out of the scope devices which rely on wired Internet connectivity (e.g. broadband via cable, DSL, etc.). Moreover, the RED rules do not ensure that a device is secure during its lifespan, as they are limited to when the product is 'placed on the market'. https://ec.europa.eu/docsroom/documents/40763/attachments/2/translations/en/renditions/native

[83] In 2020, the BEUC report "The Long and Winding Road" illustrated the current lack of effectiveness in the application of the GDPR; in particular, how the lack of harmonised binding administrative procedures to deal with cross-border complaints and the slow pace of proceedings have a negative impact on the protection of consumers. https://www.beuc.eu/sites/default/files/publications/beuc-x-2020-074_two_years_of_the_gdpr_a_cross-border_data_protection_enforcement_case_from_a_consumer_perspective.pdf

We also welcome the **increasingly active role of ENISA under the CRA proposal.** In particular, ENISA will support the European Commission when digital products present a significant cybersecurity risk, under the procedure at EU level established in Article 45. ENISA is indeed best placed to support the development of a coherent EU approach towards cybersecurity and to help ensure the protection of the privacy and security of consumers in the context of the enforcement of the CRA. That is precisely the reason why we would like **to see this role strengthened**.

Further to its established legal competences[84], the CRA proposal should also **confer a clear role on ENISA** during investigation **procedures at the national level. Article 43 should expressly mention that ENISA may assist national authorities** in the technical aspects of their investigations to check compliance with or to detect infringements of the CRA, by **conducting evaluations and assessments on the request of a national authority**, issuing non-binding opinions. **As an alternative, the creation of a highly specialised body of technical experts designated by the Commission** could also be envisaged, with the purpose of assisting national authorities with additional technical expertise. The **provision of external support** within the current framework is fundamental to ensure national authorities are **not constrained by the lack of available resources**.

In addition, to increase trust in the market and ensure a high level of consumer protection, the effectiveness and consistency of market surveillance and enforcement must be strengthened by **actively promoting a culture of information-sharing and cooperation** between all relevant actors.

For instance, it is of particular importance that **Article 41** of the CRA proposal enshrines the **need for cooperation between national supervisory authorities**, in particular in the case of a possible overlapping of competences of national supervisory authorities under the CRA and the competences of other authorities, such as the data protection authorities under the GDPR. However, in order to ensure the effective and consistent protection of consumers across the EU, clear cooperation mechanisms should be defined. Moreover, the CRA proposal should clarify to whom consumers can complain in situations of overlap and which authority should take the lead in the respective enforcement action.

More importantly, the **proposal fails to build synergies between public and private enforcement** and clear communication channels between users and national authorities. Consumers and those organisations that represent them should have access to clear complaint mechanisms to **report possible cases of non-compliance to the attention of market surveillance authorities**. This would create a '**virtuous cycle'** that would certainly contribute to **relieve the significant burden on market surveillance**, while allowing consumers to alert **authorities to take action when required**.

Close **cooperation between national market authorities and consumer protection organisations** should be encouraged. This would result in better market screening, and increased awareness and would ultimately help prevent violations of the CRA obligations.[85]

[84] ENISA competence to contribute to the development of EU policy and law in the filed of cybersecurity is established in Article 5, Regulation (EU) 2019/881 of 17 April 2019 on (Cybersecurity Act): https://eur-lex.europa.eu/eli/reg/2019/881/oj

[85] BEUC German member, Verbraucherzentrale Bundesverbands (vzbv) has recently signed, in May 2020, a Memorandum of Understanding with the German Federal Office for Information Security (BSI) where they commit to cooperate for the period of three years with the aim to work together towards raising awareness of consumers and actively preventing violations of EU law on digital consumer protection: https://www.vzbv.de/meldungen/verbraucherschuetzer-kooperieren-mit-bundesamt-fuer-sicherheit-der-it

BEUC recommendations

- **Strengthen the effectiveness and consistency** of market surveillance and enforcement, actively **promoting a culture of information-sharing and cooperation** between all relevant market actors.

- Provide for **clear cooperation mechanisms between market surveillance authorities**, especially in case of overlapping competences, and foster synergies between public and private enforcement with clear communication channels between users and national authorities.

- Ensure the European Commission is given **effective powers to timely intervene** in case of inaction by national authorities regarding non-compliance with the CRA requirements.

- **Reinforce national level enforcement on a technical level**, by establishing a clear role under the CRA proposal for ENISA to assist the action of national authorities or, alternatively, by **creating a highly specialised body of technical experts** designated by the Commission.

7. Effective remedies and means of redress for consumers

BEUC would like to reiterate how **crucial it is that consumers have access to effective remedies and means of redress**. Unfortunately, the **CRA proposal completely fails to address this point**.

There is no **clear mechanism or right for consumers to lodge a complaint with a national authority** or even an obligation for companies to provide a **complaint-handling mechanism**. The obligation established under Annex II, (2) for manufacturers to include in-product information and user instructions a reference to a **"point of contact** where information about cybersecurity vulnerabilities of the product can be reported and received" is **manifestly insufficient**.

Moreover, the proposal **fails to establish any right to redress or compensation** for affected users, or even to allow their legal representation by civil society organisations, including consumer organisations, to assist them in the exercise of their rights.

In this regard, the **CRA should be aligned with the latest EU digital legislation** such as the Digital Services Act (DSA)[86] and the Digital Market Act (DMA),[87] which contain provisions to ensure that consumers have **clear rights and effective means to seek redress** in case of **non-compliance with any of the obligations set out in these Regulations.**

Although the **Product Liability Directive (PLD) is complementary to the CRA proposal,** when it comes to the compensation for damages that a product may cause, it **is insufficient.**

A **much welcomed revision of the PLD[88] is ongoing**. However, the Commission proposal has **significant shortcomings** as it places the **burden of proof** for the defect, the damage and the causality between the defect and the damage on consumers and does not cover non-material damage, contrary to what BEUC has been calling for.[89] More

[86] https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-032_the_digital_services_act_proposal.pdf
[87] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.265.01.0001.01.ENG&toc=OJ%3AL%3A2022%3A265%3ATOC
[88] Proposal for a Directive on liability for defective products: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A495%3AFIN
[89] https://www.beuc.eu/publications/product-liability-20-how-make-eu-rules-fit-consumers-digital-age/html

importantly, the Commission proposal is limited regarding its notion of "defectiveness", with the risk of not covering all cybersecurity requirements enshrined in the CRA proposal. To determine whether a product is defective, the Commission proposal only refers to safety-relevant cybersecurity requirements which would not cover all the cybersecurity requirements set out by the CRA proposal.

To deliver **a true 'safety net' for consumers,** the CRA should ensure consumers can seek **adequate compensation** for any damage or loss caused by defective products due to violations of the obligations and cybersecurity requirements set out by the CRA.

BEUC recommendations

The CRA proposal should include**:**

- **Right to lodge a complaint before a market surveillance authority or Court**: a right for consumers to complain to a national authority or to seek judicial remedies when affected by non-compliance with the CRA.

- **Internal complaint-handling mechanism:** an obligation for companies to make a complaint mechanism available to consumers, under obligation to react to complaints within a short period of time, preferably within **a maximum of five working days.**

- **Right to compensation:** affected consumers should have the right to seek adequate redress and compensation against any damage or loss suffered due to an infringement of the obligations and requirements under the CRA.

- **Right to representation:** an article allowing consumer organisations to represent individual consumers in the exercise of their rights. Consumer organisations should also be allowed to act in the 'general interest' (i.e. be able to bring forward complaints without a mandate from an individual).

- **Adding the CRA to the Annex of the Representative Actions Directive (RAD)**[90]: a provision adding the CRA to the Annex of the RAD making it possible for consumers to benefit from collective redress mechanisms and injunctive relief when harmed due to non-compliance with the obligations of the CRA. This would also ensure greater coherence with other recent EU digital legislation (e.g. Digital Services Act, Digital Markets Act, General Product Safety Regulation) which have also been added to the scope of the RAD.

8. Final provisions

Finally, BEUC **recommends an even swifter application** than the proposed **24 months** (excluding Article 11, to apply 12 months after entry into force).

Although it is understandable that manufacturers, notified bodies and Member States should have enough time to adapt to the new requirements, there can be **no technical justification to further delay the application of these rules for a long period of time**. This is especially clear when comparing the CRA to other similar legislation just recently adopted. For instance, both the DSA and the DMA, more complex pieces of digital legislation, have a shorter application period of 15 months after entry into force.

[90] 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: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32020L1828

BEUC recommendations

- Amending Article 57 to **harmonise the date of application of the CRA proposal, reducing it to match the 12 months** after the date of entry into force already proposed for the reporting obligations on manufacturers under Article 11.

-ENDS-

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.