Raising standards for consumers

POSITION PAPER

ANEC Response to EC Call for Evidence for an Impact Assessment on the Cyber Resilience Act (CRA) initiative

Contact: Chiara Giovannini

Chiara.Giovannini@anec.eu

ANEC is supported financially by the European Union & EFTA

Ref: ANEC-2022-DIGITAL-CYBER-006 25/05/2022

European Association for the Co-ordination of Consumers Representation in Standardisation aisbl

Rue d'Arlon 80 – 4th Floor - B-1040 Brussels, Belgium
T: +32-2-7432470 / anec@anec.eu / www.anec.eu

INTRODUCTION

ANEC is the European consumer voice in standardisation, defending consumer interests in the processes of technical standardisation and conformity assessment, as well as related legislation and public policies.

Consumers are key stakeholders and ANEC is pleased to provide the results of its consultations with its members, national consumer organisations in 31 countries and technical experts, to answer the European Commission call for evidence on the impact of the proposed Cyber Resilience Act (CRA).

ANEC supports the broad scope of the initiative and agrees that a robust and coherent EU legislative intervention on cybersecurity will provide a more effective, less-fragmented protection for consumers. ANEC agrees that the CRA will complement and close gaps in the existing EU legislative framework.

Given the fast-moving rate of change, ANEC calls for swift action and in-depth intervention to keep consumers safe and secure and address challenges posed by the emergence of new technology products such as apps and connected devices.

1 | ANEC Views

ANEC is pleased to share its views on current and emerging problems related to the cybersecurity of digital products and associated services, including non-embedded software.

Cyber security risks are increasing for consumers. The fast-growing omnipresence of digital products and services in the car, home, transport, almost constantly on and around the consumer significantly increases the risks, **irrespective of the consumer's age or ability to consent, to regularly upgrade or to defend their privacy, data and finances**.

While the rate of technological advances and consumer take-up has been and continues to be extremely fast, existing EU legislation does not yet appropriately or **fully address the cybersecurity aspects of tangible and intangible digital products throughout their lifecycle.**

Safer and more secure products lead to greater confidence in the Single Market[1]. There is a problem with the **vulnerability of products**, due to the consumers fair and legitimate assumptions that products and services on sale are secure, when in fact they are mostly unsecure.

The majority of products are designed without in-depth consideration of cybersecurity risks. These **risks need to be factored in at the beginning of the design phase and continually assessed during the full lifecycle of the product**.

Consumers need clarity as the current situation leads to difficulty in product comparison. Why are they potentially paying more for a certain product? Are the benefits outweighing the high costs or not?

Consumer organisation testing over the years has **repeatedly found that the market has not self-corrected** and that there is still a low-level of cybersecurity of digital products and associated services[2]. There is an urgent need to radically **raise the security levels to strengthen defences against existing and emerging cybersecurity incidents**.

The Hackable Home Campaign tested smart devices in consumers' homes. **Between half to two-thirds of tested products had a significant security flaw and could be hacked remotely**[3].

ANEC is concerned about the lack of vendors informing consumers about the risks at the point of sale or after. ANEC has stressed that **consumers should not bear**

[1] ANEC BEUC GPSR position paper 'Keeping consumers safe from dangerous products: How to make the General Product Safety Regulation a useful tool to ensure product safety' Ref: BEUC-X-2021-107 - ANEC-WP1-2021-G-054 -15/11/2021

[2] 23 June 2017 The hackable home: investigation exposes vulnerability of smart-home devices – Which? Press Office and Sept 2018 Consumentenbond, "A house full of clever spies" consumentenbond.nl

[3] BEUC press release https://www.beuc.eu/publications/eu-cybersecurity-strategy-paves-way-much-needed-rules-better-secure-connected-products/html

the burden of cybersecurity protection and should be informed in an easy-to-understand way about the risk of the product for intended and foreseeable use[4].

ANEC is concerned about the absence of information for consumers to make informed purchases. For example, would a parent purchase a doll for their child if they knew it could spy, collect private data or be controlled remotely and speak to their child[5]?

Consumers are faced with risks to their finances by phishing scams and ransomware. **ANEC believes that the burden should not fall on the consumer** to ensure that products and services are cybersecure.

Consumers investing in modern (physical) property protection products such as smart locks, security cameras & house alarms etc, which **lack horizontal cybersecurity standardisation**, may even expose their homes to more to risks.

ANEC notes the **security and fundamental rights concerns around the increased use of biometrics**, fingerprint and facial recognition access. A double-edge sword, biometrics have the benefit of making products and systems secure and easily accessible by consumers, yet have more dangerous consequences if hacked. Consumers must have the right to chose or not to use biometrics and still be able to securely access a product or service. The systems should not be designed by default to give secure access only if consumers use their biometric data.

Legislative intervention is clearly needed and **the role of Harmonised Standards, providing presumption of conformity to the legislation**, should also be stressed.

[4] Requirements for ICT Products (ANEC-2021-DIGITAL-CYBER-004)
[5] Cayla the spying doll clip, Norwegian Consumer Council

2 | ANEC Recommendations

ANEC is pleased to share its recommendations on the possible policy approaches to address such problems, the available options and their potential impacts.

ANEC supports Option 5, Horizontal Legislation.

ANEC supports an all-encompassing policy approach, in that the full scope of consumer products and services should be covered by a robust CRA.

ANEC recognises that articles in existing legislation partly address cybersecurity issues and a coherent legislation is required to avoid gaps and provide clarity for industry[6]. **Regulations concerning consumer security should always be introduced as horizontal legislation**.

ANEC supports introducing **mandatory horizontal cybersecurity requirements** for hardware, software, services and ancillary services, wired and wireless, embedded and non-embedded digital products with security **by default and by design** as the most encompassing protection for all European consumers.

ANEC reiterates that the role of Harmonised Standards, providing presumption of conformity with the relevant legislation, should also be stressed. In combination with a risk-based approach, tailored solutions for a wide range of product areas and safety and security requirements can be developed in a cost-effective and efficient way.[7]

ANEC supports mandatory requirements to protect consumers and be a level playing field for companies.

ANEC has elaborated a list of requirements from a consumer point of view, calling for a **distinction to be made between technical and organisational requirements**.

ANEC is not against promoting the use of biometrics that clearly follow related standards and regulations. Organisations that use biometrics should have a higher level of security. The biometrics offered shall not be "black box" biometrics, but the providers must clearly state which standards and regulations they follow and be open to scrutiny. The use of biometrics must be entirely voluntary and not be a reason not to increase baseline requirements. There must always be a clear option for consumers to have secure access by using other authentication methods.

ANEC believes that products/services must be 'fit for purpose', which in this case would be fit for cyber security protection. They must be created cybersecure by design and by default so that they are safe and **ready to use by the consumer for the duration of the life cycle**, just like a car comes with a pre-installed airbag, ready to use when necessary.

[6] The European Commission mentioned the horizontal legislation in its Cybersecurity Strategy, published in December 2020. ANEC welcomed these developments as they meet our long-standing request of cybersecurity legislation on IoT devices.
[7] May 2021, ANEC replies to EC Study on the need of Cybersecurity Requirements for ICT Products…Q14.

ANEC believes that product manufacturers and suppliers should exercise a duty of care throughout the product's lifecycle. It is important to cover the whole lifecycle and require vendors to make information available, provide instructions on securely installing, operating and using the product/service in question. The length of time depends on the product and the different risks related to the product throughout its lifecycle. Vendors should also be required to take corrective actions (such as patching, recalling or withdrawing a product) when a product is found to be unsecure. If a product is discontinued or withdrawn, updates and information must remain available to consumers for a minimum of five years.

In ANEC's view, there also needs to be very effective sanctions and market surveillance if false claims are made and unsecure products are put on the market. ANEC asks for strong enforcement mechanisms and clear provisions on remedies and means of redress for consumers when obligations are not respected.

ANEC supports a generic technology-neutral security objectives approach to risk assessment. ANEC supports taking into account the functionality, the societal importance, the intended and foreseeable use and the risk associated with a product. Consideration should be given to the different risk levels given the different knowledge and ability of users e.g., less tech-savvy or children.

ANEC supports the determination of risk and risk categorisation associated with a product being carried out by a competent authority, an independent body responsible for verifying compliance with the cybersecurity requirements and legislation.

The manufacturer may not know or for commercial reasons, not wish to inform the consumer of the risks.

ANEC recommends that consumers have flexibility to upgrade or downgrade and a minimum provision of software support[8]. Consumers must have the option to upgrade or downgrade their operating system version at any time, going back to the functionalities they originally paid for. Any security vulnerability or potential impact on performance must be communicated but the installation/de-installation should always be possible. Consumers should also have the option to remain in an older operating system version but still install the latest security updates.

ANEC supports addressing market access requirements and the risks of lack of security at the European level[9]. ANEC agrees on the need of mandatory baseline requirements to protect consumers and be a level playing field for companies.

ANEC recommends increasing EU consumer consultation in EU policy decisions and greater consumer representation and input in the standardization process. In its work on standards, ANEC regularly sees the interests of non-EU manufacturers powerfully influencing and determining requirements for European and international

[8] ANEC comments on ETSI TC-EE & TC CYBER Ecodesign and Energy labelling requirements for mobile phones and tablets (ANEC-DIGITAL-2021-G-122)

[9] ANEC spoke at the ENISA certification conference during the panel IofT Certification, 02/12/2021 (ANEC-DIGITAL-2021-G-151).

Standards[10]. ANEC experts work to represent the views of European consumers, yet it is not easy to tilt the balance of power and influence in favour of the welfare of European citizens.

ANEC agrees with the European Commission that the EU should strive to become a leader in cybersecurity by self-determining a full package of robust and horizontal requirements that can best serve and protect the interests and rights of its citizens and consumers.

ENDS.

[10] ANEC Position paper on 'The role of standards in meeting consumer needs and expectations of AI in the European Commission proposal for an artificial Intelligence Act', 01/12/2021 (ANEC-DIGITAL-2021-G-141).

ANEC is the European consumer voice in standardisation, defending consumer interests in the processes of technical standardisation and the use of standards, as well as related legislation and public policies.

ANEC was established in 1995 as an international non-profit association under Belgian law and is open to the representation of national consumer organisations in 34 countries.

ANEC is funded by the European Union and EFTA, with national consumer organisations contributing in kind. Its Secretariat is based in Brussels.

Designed by AdGrafics.eu

ANEC

Raising standards for consumers

European association for the coordination of consumer representation in standardisation aisbl

Rue d'Arlon 80, box 3
B-1040 Brussels, Belgium

+32 2 743 24 70
@anectweet
anec@anec.eu
www.anec.eu

EC Register of Interest Representatives:
Identification number 507800799-30

BCE 0457.696.181

ANEC is supported financially by the European Union & EFTA