*Raising standards for consumers*

The Consumer Voice in Europe

# KEEPING CONSUMERS SECURE

## How to tackle cybersecurity threats through EU law

**Contact: Frederico Oliveira Da Silva – digital@beuc.eu**

Ref: BEUC-X-2019-066 - 05/11/2019

**ANEC, THE EUROPEAN ASSOCIATION FOR THE CO-ORDINATION OF CONSUMER REPRESENTATION IN STANDARDISATION**
Av. de Tervueren 32, box 27 – 1040 Brussels - +32 (0)2 743 24 70 - www.anec.eu
EC register for interest representatives: identification number 507800799-30

**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

Funded by the European Union

## Why it matters to consumers

With the Internet of Things[1], the number of connected devices and digital services is skyrocketing and interconnectivity between products is reaching all sectors of society, including transport, health, banking and energy. While digitalisation provides many benefits for consumers, the risks and challenges it brings are equally important, if not even greater. Ensuring cybersecurity is precisely one of the most fundamental challenges we face.

## Summary

### 1. INTERNET OF THINGS

- The European Commission should propose a new horizontal cybersecurity law which establishes mandatory minimum security requirements. This law would apply horizontally to all consumer products and its associated services[2] provided that sector specific legislation doesn't take precedence.
- Such law should have strong enforcement provisions. These rules should enable national authorities to remove insecure products from the market as well as allow consumers to benefit from remedies (e.g. compensation).

### *1.1. Security by design and by default: baseline security requirements for a new EU cybersecurity law*

From their very inception products and services should include high-level cybersecurity functionalities ('security by design'). Their default settings must always be the secure ones ('security by default').

[1] Internet of Things: combination between the connected products which are intended to be used by consumers (e.g. connected toys, smart watches, baby monitors, smart home appliances such as smart door locks or smart thermostats) and the associated services for such products (e.g. mobile apps linked to the product).

'Associated services' are considered as the digital services that are necessary for the functioning of the IoT devices, for example, mobile applications, cloud computing/storage and third-party Application Programming Interfaces (APIs).

This definition is identical to the one used in the UK's Code of Practice for Consumer IoT Security

[2] Please see previous footnote for definition of 'associated services'

### a. Security updates

- At the time when they are placed on the market, connected products and their associated services must be protected against any known vulnerabilities.
- Security updates should be provided by the manufacturers and service providers during a minimum period of time (depending on the expectations of the consumer and the expected lifespan of the product and its associated service).
- The manufacturers and service providers' end-of-life policy must be clear to the consumers at the time of the purchase. Such policy shall explicitly mention the period until which security updates will be provided.[3]
- Consumers should be informed about the different possibilities once the manufacturer is no longer supporting the product (e.g. disconnect from the internet; dispose it in a responsible way).
- Manufacturers and service providers must ensure that consumers can easily install their security updates, including those who are not tech-savvy.
- In exceptional circumstances where there is a safety risk to the consumers (e.g. when using a self-driving car), security updates can be installed automatically provided that certain conditions to protect the consumers autonomy and privacy are met.

### b. Strong authentication mechanism

- Connected products intended for consumers should by default only include high-security authentication features.
- For products and associated services which use a password, the default password must be unique and contain a certain level of complexity and length. If consumers can create their own passwords, those must meet high security features.

### c. Encryption

- All manufacturers and service providers should ensure that the data stored in their services as well as the data stored by their connected products is properly encrypted in accordance with current best practices.
- The communication between consumer IoT devices, IoT devices and the servers, the manufacturer/service provider and the third parties should be encrypted as well.
- They should also ensure that third parties that access the data are keeping it properly encrypted.

### d. Cybersecurity Labels

- Before the establishment of a cybersecurity label under the ENISA certification scheme, the EU Cybersecurity Agency (ENISA), should provide for preliminary qualitative testing of such labels to ensure they are well designed and tested for effectiveness, so that end-users correctly understand the meaning of the label.
- If a label is established under a certification scheme, national cybersecurity certification authorities need to be equipped with the necessary financial and human resources to perform their tasks and ensure compliance of the label with the scheme.

---

[3] As mentioned in Chapter 1.1, the Cybersecurity Act obliges manufacturers and service providers of *certified* products and services to provide cybersecurity information, including information on the period during which they provide security support (i.e. security updates).

### e. Isolation of critical systems

During the design and production process, manufacturers should guarantee that the critical systems of certain connected products are isolated from the rest of the products' internal network and thus avoid vulnerabilities to spread from one system to the other. (e.g. vulnerability in the DVD system should enable malicious actors to take control of the car).

### f. Vulnerability disclosure policy and security oversight

- Manufacturers and service providers must have a 'contact point' through which researchers or users can submit the vulnerabilities they discover.
- Manufacturers and service providers must continuously monitor the security of their products and services.

### g. Notification of a cybersecurity breach to consumers

- Whenever a security breach may have a serious impact on consumers , manufacturers and service providers shall inform their users without undue delay and provide them with the necessary information to mitigate the adverse effects of the breach.

### h. Cybersecurity and repairability

- Consumers should have a right to repair and modify their products to address security vulnerabilities when the manufacturer is no longer providing security updates.

### i. Appropriate response in case of cybersecurity breach

- When safety-critical functions of a device are compromised due to a cybersecurity attack, the device should respond appropriately and without causing any harm.
- If a product or service is forced to unexpectedly disconnect due to a cybersecurity incident, it must do so in a safe and responsible fashion. The features of a device that in theory do not require connectivity should continue to work when the product or service is not connected to the internet (e.g. the lack of connectivity of a smart lock should not prevent someone from opening his door)

## *1.2. **Standardisation** (ANEC and BEUC demands):*

- For a standard to be effective, its requirements need to be clear, unambiguous and replicable.
- The European Commission and the European Standardisation Organisations (ESOs) should step up their efforts to develop European standards on security of connected products, with the contribution of all concerned stakeholders' expertise. We recommend a collaborative approach on standards in this area, with an agreement between the ESOs to define which organisation will be responsible for which activities.

# 2. ROLE OF ENISA

- ENISA should pro-actively work towards promoting an EU cybersecurity policy that addresses needs and concerns of and for consumers. This means that the consumers' needs are taken into account regularly and systematically in the relevant cybersecurity policies and that ENISA adapts its work programme to give more space to activities to achieve this objective.

- ENISA should actively promote the co-operation between the different national authorities that have to deal with cybersecurity issues. These are at least the data protection, telecoms and consumer protection authorities.
- ENISA should ensure a balanced representation between the different stakeholder groups within ENISA's stakeholder bodies.

## 3. DIRECTIVE ON SECURITY OF NETWORK AND INFORMATION SYSTEMS (NIS DIRECTIVE)

The Directive requires major infrastructure providers to make sure their facilities are resilient against online security threats. In this context, the European Commission must ensure that the implementation of the NIS Directive, in particular the selection of operators of essential services, is consistent all across the EU.
Although the Directive only applies to large companies, every piece of infrastructure, however small, that is not secure poses risks to the wider system. This is why a reform of the NIS Directive must ensure that smaller operators fall under its scope. This can be done by an extension of the scope of 'Operators of Essential Services' or by the introduction of a new definition. A review of the NIS Directive should include social media platforms in the definition of 'Digital Service Providers'.

## 4. CYBERSECURITY INCIDENT REPORTING

The European Commission shall put in place a common cybersecurity incident reporting system that ensures a timely notification to consumers in all circumstances. The notification to consumers shall include information that will enable them to mitigate the adverse effects of the incident.

## 5. CYBERSECURITY LEGISLATION MAPPING

In order to define the scope of the new legislation and to address the gaps in specific product or services legislation with security aspects, the European Commission should provide a detailed mapping of relevant security legislation with an evaluation regarding its effectiveness to protect consumers, citizens and the entire society from security flaws.

# Contents

# 1. Introduction

## An insecure digital environment

According to recent estimates, there will be up to 25 billion connected devices by 2021.[4] Many cybersecurity experts[5]-[6]-[7] attest that the Internet of Things is fundamentally insecure with too many products lacking the most basic security features.

Consumer organisations' testing has shown that many connected products available on the market come with multiple risks and basic flaws.

A campaign by our Norwegian member Forbrukerrådet launched in December 2016 – #ToyFail[8] – looked at the technical features of popular connected toys sold on the EU market. Forbrukerrådet discovered that with a few simple steps anyone could connect to a children's doll named Cayla, one of the connected toys tested, and speak to the kids using the toy, thus putting the child's physical and privacy safety at risk. A second Norwegian campaign (#WatchOut[9]), which was launched in October 2017, tested the security features of smart watches whose main function is to enable parents to keep in touch with their children and track their real-time location. Again, Forbrukerrådet discovered serious security flaws in these devices, including the possibility for an attacker to easily change the geo-location of the watch ('location spoofing'[10]) as well as track and contact the child directly.

In May 2018, our Belgian member, Test Achats/Test Aankoop, installed 19 popular smart devices in a house (including a fridge, an alarm system, a thermostat, a printer, a children's tablet, a door lock, a speaker and a vacuum cleaner robot) and challenged two ethical hackers to find security vulnerabilities within a specific time period. Just within 5 days, more than half of products were considered to be vulnerable.[11]

In recent campaigns, Which?[12], Stiftung Warentest[13], OCU[14] and Consumentenbond[15], consumer organisations from the United Kingdom, Germany, Spain and The Netherlands respectively, found similar security flaws in other consumer connected products.

Another important aspect for consumers when it comes to cybersecurity is data breaches. A significant portion of internet of things devices and digital services (e.g. online platforms or mobile apps) are collecting significant amounts of user data. This information is often used to improve and individualise services, or for advertising purposes. The collection, processing and storage of these vast amounts of user data can be problematic from a data protection point of view and adds significant risks when coupled with poor cybersecurity

---

[4] Ref.: https://tech.economictimes.indiatimes.com/news/corporate/25-billion-connected-things-will-be-in-use-by-2021-gartner/66563141?redirect=1
[5] Ref.: https://www.stiftung-nv.de/de/publikation/internet-insecure-things
[6] Ref.: https://www.pentestpartners.com/security-blog/why-is-consumer-iot-insecure/
[7] Ref.: https://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/
[8] Ref.: https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/
[9] Ref.: https://fil.forbrukerradet.no/wp-content/uploads/2017/10/watchout-rapport-october-2017.pdf
[10] A spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data, thereby gaining an illegitimate advantage (Definition from Wikipedia)
[11] Ref.: https://www.test-achats.be/action/espace-presse/communiques-de-presse/2018/hackable-home
[12] Ref.: http://press.which.co.uk/whichpressreleases/which-issues-child-safety-warning-on-connected-toys/
[13] Ref.: https://www.test.de/Smart-Toys-Wie-vernetzte-Spielkameraden-Kinder-aushorchen-5221688-0/
[14] Ref.: https://www.ocu.org/organizacion/prensa/notas-de-prensa/2017/juguetes-conectados-201217 and https://www.ocu.org/consumo-familia/bebes/noticias/juguetes-conectados-wifi
[15] https://www.consumentenbond.nl/nieuws/2019/deel-beveiligingscameras-te-hacken and https://www.consumentenbond.nl/beveiligingscamera/test-slimme-deurbellen

practices. When companies collect troves of user data, this increases the possibility of data breaches that could potentially put consumers at risk.

In October 2018, British Airways revealed that approximately 380,000 transactions had been compromised due to poor cybersecurity measures. The data stolen included log in, payment card, and travel booking details as well name and address information. This data breach eventually led to an intervention from the Information Commissioner's Office (ICO) and a record fine of £183 million.[16] And in the U.S. alone, over 16 million U.S. consumers fell victim to identity theft in 2016, costing them $ 16 billion.[17]

## Consumer IoT: a hazard for consumers…

In what concerns the Internet of Things, lack of cybersecurity can have serious consequences for both consumers and for society at large due to the impact on the infrastructures that are critical for the functioning of for example hospitals, power grids, transport networks and financial institutions.

Seemingly harmless connected devices such as an electric kettle or lightbulb can allow hostile actors to extract valuable information that gives access to critical information such as a home Wi-Fi key. Similarly, compromised devices such as connected toys or cameras can pose risks of surveillance or blackmail, while hackable medical equipment[18] and cars could have potentially fatal consequences.

It is also important to note the long-term impact that cybersecurity vulnerabilities can have for example on children.[19] Recent examples have shown malicious hackers exploiting the vulnerabilities of baby monitors for the sole purpose of scaring the children.[20]

## … but also for critical infrastructure

In an interconnected ecosystem such as the Internet of Things, a chain is only as strong as its weakest link and a vulnerability in a connected product can have a significant impact on critical infrastructure. In 2008, hackers accessed the control system of an oil pipeline in Turkey. It was later discovered that the entry point in the oil infrastructure was a vulnerability in the surveillance cameras.[21]

Moreover, if many connected devices are compromised to create a so-called botnet, hackers can seize control and coordinate attacks on critical infrastructure. For example, if a botnet consisting of thousands of insecure smart meters is used to overload the traffic of a power grid, it can cause the server to crash. In the worst-case scenario, this means that insecure consumer products could be used as attack vectors that threaten national security interests. In October 2016, a massive attack used hundreds of thousands of insecure consumer devices infected with a specific malware called Mirai to disrupt the internet and bring down websites such as Twitter, Amazon, Spotify and Netflix.[22] In the same year, a botnet attack halted the heating distribution of two buildings in Finland amidst freezing winter temperatures.[23] It is also important to underline that in the case of a botnet

[16] Ref.: https://www.bbc.com/news/business-48905907
[17] Ref.: https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin
[18] Ref.: https://arstechnica.com/information-technology/2017/08/465k-patients-need-a-firmware-update-to-prevent-serious-pacemaker-hacks/
[19] Ref.: https://ec.europa.eu/jrc/en/news/why-we-need-manage-internet-toys
[20] Ref.: https://www.computerworld.com/article/2476196/hacker-strikes-again--creep-hijacks-baby-monitor-to-scream-at-infant-and-parents.html
[21] Ref.: https://arstechnica.com/information-technology/2014/12/hack-said-to-cause-fiery-pipeline-blast-could-rewrite-history-of-cyberwar/
[22] Ref.: https://www.test.de/Schadsoftware-Das-Internet-der-Dinge-infiziert-5249226-0/
[23] Ref.: https://metropolitan.fi/entry/ddos-attack-halts-heating-in-finland-amidst-winter

attack consumers are not aware that their connected device has been compromised and being used to disrupt a service. This makes it harder for consumers to protect against this.

### Lack of incentives for manufacturers and service providers to enhance security

Several elements explain the general lack of security of smart products and related services. For many manufacturers and service providers, their primary aim is to place their product on the market as fast as possible ('short time to market') and security only comes as an afterthought. Also, manufacturers and vendors who have traditionally sold toothbrushes and dolls are unlikely to have the necessary competence to ensure cybersecurity when they move into the Internet of Things. They often fail to account for possible cybersecurity issues when importing and reselling connected products. Finally, and maybe most importantly, the manufacturers' or sellers' liability for damages caused by a lack of security in consumer IoT is legally not clearly established. Responsibility for security is thus not incentivised by legal liability.

### Consumers are concerned with the security of their connected products

According to a recent study from our Norwegian member Forbrukerrådet three out of four consumers in Norway are concerned about cybersecurity and privacy in smart products.[24] A study[25] from the UK Government also revealed that when purchasing a new consumer IoT product, 'security' is the third most important information category (higher than privacy). For those who didn't rank 'security' as a top-four consideration, 72% said that they expected security to already be built into devices that were already on the market. This last figure shows that there is currently a gap between what consumers think they are buying and what they are actually buying.

In this paper, we will assess the current EU framework applicable to connected products, identify its main shortcomings and propose policy measures to ensure that consumers are protected from cybersecurity threats (Chapter 1). In Chapter 2, we will focus on the NIS Directive. Finally, we will address the issue of cybersecurity incident reporting in chapter 3.

[24] Ref.: https://www.forbrukerradet.no/side/consumers-dont-trust-connected-devices/
[25] Ref.: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/798543/Harris_Interactive_Consumer_IoT_Security_Labelling_Survey_Report.pdf

## 2. Internet of Things

When it comes to the security of connected products, the EU regulatory framework is fragmented and unclear.

### 2.1. Shortcomings of the EU legal framework

#### 2.1.1. Cybersecurity Act: a missed opportunity

The recently adopted Cybersecurity Act[26] represented a possible regulatory opportunity to address cybersecurity problems in connected products. This Regulation creates a framework for the establishment of European certification schemes for ICT products, services and processes.

While we support the introduction of a framework for an EU cybersecurity scheme, we have expressed[27] doubts about the effectiveness of the adopted instrument due to its *voluntary nature*. Without a binding framework, there is no guarantee that companies will adhere to a certification scheme and that the overall security of connected products will increase.

Furthermore, it remains to be seen whether a certification scheme aimed at addressing the security vulnerabilities of connected products intended for consumers will eventually be put in place.[28] Under Article 47 of the Cybersecurity Act, the priorities for future certification schemes will be published by the European Commission in a Union rolling work programme. If connected products will feature in this work programme remains to be seen.

From a consumer perspective, an important point in the Cybersecurity Act is the provision on 'Cybersecurity information for certified products'. According to Article 55, *if* manufacturers and service providers certify their products and services they must make cybersecurity information, including information on the period during which security support (i.e. security updates) will be offered to end users, publicly available to consumers.

This sort of information is useful as it should enable consumers to make an informed purchase decision. It remains to be seen however how the information will be made available: the relevant Recital from the Cybersecurity Act only obliges this information to be available online and not in physical form. Furthermore, it is also important to understand how this provision will be used in combination with the provision establishing the possible use of labels (Article 54 (1) i)).[29]

#### 2.1.2. Product safety legislation: focus on mechanical and chemical safety

Thanks to the General Product Safety Directive and sector-specific legislation such as the Radio Equipment Directive or the Toys Safety Directive, manufacturers are obliged that any product put on the market is safe. However, the concept of 'safety' is too narrow and fails to protect consumers from the security flaws which come along with connected devices thereby jeopardising the safety of the users.

---

[26] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

[27] Ref.: https://www.beuc.eu/publications/beuc-x-2018-017_cybersecurity_for_connected_products.pdf

[28] The Regulation for a Cybersecurity Act was published on 7th June 2019 in the Official Journal of the European Union. It entered in force on the 27th June 2019.

[29] For more information on labels, please see page 16

This is because product safety is understood in the traditional sense only with regard to their potential harm to consumers' health and physical integrity, such as through exposure to harmful chemicals and physical injuries. This concept of product safety is outdated knowing that devices which can connect to the internet can be hacked, thereby creating new risks.

While the EU has recently updated its market surveillance legislation, the new rules[30] will not be sufficient to enforce the current product safety rules. Product safety laws and market surveillance laws are two sides of the same coin and just addressing one of them will not enable authorities to keep consumers fully safe.

### 2.1.3. Radio Equipment Directive (RED): the intermediary solution?

The Radio Equipment Directive[31] can be perceived as the quick intermediary solution to fix some of the problems with connected devices. Firstly, the definition of Radio Equipment is broad and encompasses a significant number of consumer connected products.[32] Secondly, it can force manufacturers to incorporate relevant cybersecurity safeguards such as the protection of personal data.[33] Thirdly, it has the proper market surveillance mechanisms in place to withdraw these products from the markets.[34]

However, while the Directive has been in force since 13 July 2017, some of its provisions, including those related to cybersecurity, need a complementary EU secondary act (so-called delegated act) to be fully applicable and effective.

BEUC has been long calling for the adoption of this delegated act. Recently, the European Commission started its preparatory works towards the adoption of these delegated acts.[35] If adopted, they acts can force manufacturers of connected products to incorporate safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected as well as to ensure the protection from fraudulent activities such as ransomware.

Overall, the Radio Equipment Directive can play an important role in increasing the security of connected products. However, it is important to note that the Directive will not ensure the security by design and by default of all connected products intended to consumers. For example, exclusively *wired* connected products fall outside of the scope.[36]

Another shortcoming of the Radio Equipment Directive is related to the structural design of the 'New Legislative Framework'.[37] By imposing obligations on the manufacturers at the time when the *product is placed on the market*, the Directive focuses on the period in which consumers purchase the product whilst ignoring the dynamics of cybersecurity: a secure

---

[30] EU Regulation on Market Surveillance and Compliance of Products: see recital 30, https://data.consilium.europa.eu/doc/document/PE-45-2019-INIT/en/pdf
[31] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC
[32] Article 2 (1) 1) Radio Equipment Directive
[33] Articles 3 (3) d), e) and f) Radio Equipment Directive
[34] Chapter V of the Radio Equipment Directive
[35] Article 3 (3) e) and f) Radio Equipment Directive
[36] Internal legal research conducted for BEUC by Institut für Recht der Netzwissenschaften (IRNIK)
[37] The New Legislative Framework' or 'NLF' is the EU legal framework on non-food product compliance. The functioning of this framework is better explained in the European Commission's 'Blue Guide' on the implementation of EU product rules: https://ec.europa.eu/growth/content/%E2%80%98blue-guide%E2%80%99-implementation-eu-product-rules-0_en

product can become insecure over time (e.g. faulty update or new vulnerabilities are discovered).

### 2.1.4. General Data Protection Regulation (GDPR): limited impact on product/services security

Article 32 of the GDPR prescribes that all companies processing personal data shall implement appropriate and technical measures to ensure a level of security appropriate to the risk. These measures include the pseudonymisation of data and other well-known security principles better known as the CIA triad (ensuring the confidentiality, integrity, availability and resilience of processing systems).

If the manufacturer of a connected product does not comply with these rules, the data protection authorities can for example force them if certain conditions are met to stop the processing of the personal data. The GDPR can help to significantly reduce the risks for privacy as well as other risks related to the safety or property of the user (e.g. if strong authentication mechanisms are implemented to ensure the security of processing, harmful attacks are made more difficult regardless of whether the final purpose is to access data or break in to someone's home).[38]

The GDPR has nevertheless several limits. First, its rules are primarily aimed at addressing problems related to the protection of personal data and do not ensure the full protection of consumers beyond data protection. There are connected products in which personal data is not processed at all.[39]

Secondly, from an enforcement perspective, the GDPR does not enable for consumer redress and public enforcement intervention measures such as the withdrawal of the product form the market.[40]

### 2.1.5. Product Liability Directive: not fit for the challenges of the digital environment

Another important point is the issue of liability: what happens if a smart lock is hacked by burglars and or if a connected and automated car crashes due to a cybersecurity attack?

Currently, the legal uncertainty as regards who is liable for any harm caused by connected products is high. At the EU level, the only law applicable to the liability of connected products is the Product Liability Directive from 1985. The directive is outdated and shows many shortcomings:

First, it is not clear whether the Directive covers defects other than those causing safety issues. According to Art. 6, a product is 'defective' when it does not provide the "*safety which a person is entitled to expect*". As explained above, in product safety legislation, the concept of safety is interpreted as covering only threats to the physical safety.

Second, the definition of liable persons under the Directive is not appropriate. The Directive focuses only on 'manufacturers' without mentioning other professionals who can also be responsible for a lack of safety in case of connected products (e.g. the creators of an app which goes with such a device). Then, there is a problem about how to identify the liable person when the same product is made by several manufacturers and contributors.

[38] IRNIK research – p. CVII
[39] IRNIK research – p. CVIII
[40] IRNIK research – p. CVIII

Finally, a big problem for consumers is the need to prove the damage, the defect and the causal relationship between the defect and the damage. This can be problematic in the case of consumer IoT products: these products are by definition part of a wider network – the Internet of Things – which makes the origin of the problem difficult to identify by the average consumer.

Today, consumers have no legal certainty when their connected products cause harm due to a cybersecurity flaw. It is high time to replace the current liability regime with a modern and fair one that takes into account the most recent market developments. It must ensure that since the moment of the purchase it must be clear who is responsible for providing the updates and who is liable if something goes wrong (seller, manufacturer, software provider). The burden cannot rest on the consumer.

**DIGITAL HEALTH AS MEDICAL DEVICES**

Both the Medical Devices Regulation (MDR) and the In Vitro Diagnostic Devices Regulation (IVDR) are expected to strengthen consumers safety when using digital health solutions intended for medical purpose. For devices that incorporate software or for software that are devices in themselves, the MDR requires that the software shall be developed and manufactured in accordance with the state of the art taking into account the principles of development life cycle, risk management, including information security, verification and validation. MDR provisions also oblige the manufacturers to set out minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, necessary to run the software as intended.

Once applicable, MDR and IVDR are expected to significantly strengthen consumer protection and security of their data while using digital health solutions qualified as a medical device. However, there is a need to provide further detail on what is considered a minimum IT security standard and how manufactures should ensure it. BEUC therefore calls on the EU to ensure that the provision on minimum requirements are implemented in full respect of the principles of security by design and by default.

### 2.2. The need for a new horizontal EU Cybersecurity Law

The above short assessment shows how the current EU framework is deeply fragmented, complex and inadequate. The consequence is that dangerous products remain on the EU market.

Clearly the current situation is not acceptable, and it is key that the EU framework is adapted to ensure that all connected products intended for consumers are secure by design and by default. This is only possible with the adoption of a new horizontal regulatory instrument that implements a set of cybersecurity baseline security requirements.

It is important to clarify that any new cybersecurity horizontal law would act as 'safety net' towards other existing EU laws. In other words, similar to the role of the General Product Safety Directive and in full respect of the principle *lex specialis derogat lex generalis*, such new law would only apply when no other law is applicable or in case the more specific law has loopholes.

Another important point that this law needs to address is market surveillance and enforcement policies. Two years after the #ToyFail campaign from our Norwegian member

exposed connected toys with serious security flaws, these are still being sold on the EU market. Those retailers who removed these products from the market did so on a voluntary basis. Only the German market surveillance authority requested the destruction of these products[41]. It is important to highlight however that this request was not based on product safety legislation but rather on a national anti-espionage act and that absurdly consumers were held liable if they did not destroy the connected doll.

A public enforcement market surveillance system needs to be established with the appropriate powers to force manufacturers to remedy products or to withdraw them. An EU wide network of national authorities must be put in place to ensure that the problems related to insecure products and associated services can be addressed quickly and coherently at an EU level.

**BEUC demands:**

- The European Commission must propose a new horizontal cybersecurity law which establishes mandatory minimum security requirements. This law would apply horizontally to all consumer products and its associated services provided that no more specific provisions are being made in sector specific legislation.
- Such law should have strong enforcement provisions. These rules should enable national authorities to remove insecure products from the market and to sanction manufacturers who do not meet the security standards. In case of security flaws, consumer should benefit from remedies (e.g. compensation).

## 2.3. Security by design and by default: baseline security requirements for a new EU cybersecurity law

We enumerate below some basic principles that should underpin the security features of every consumer connected device and its associated service.

### 2.3.1. Security updates

When consumers use a connected product such as a mobile phone, a smart TV or a connected toy, they have the right to a product that is as secure as possible considering the state of technology at the time. Many cyberattacks are only possible precisely because the security protections of connected products are inadequate or outdated.

The question of security updates raises several important questions for consumers.

First, manufacturers shall make sure that when they first put a product on the market, the software that runs on the product is as secure and up-to-date as it can be according to best practices.

Secondly, manufacturers and service providers must provide the necessary security updates in a swift and efficient manner during a minimum period of time which shall take into consideration the expectations of the consumer and the expected lifespan of the product. For more durable products (e.g. smart fridges, connected and automated vehicles), security updates should be provided for longer.

[41] BBC, *German parents told to destroy Cayla dolls over hacking fears*, 17 February 2017: https://www.bbc.com/news/world-europe-39002142

Thirdly, consumers should be informed at the time of the purchase about the end-of-life policy for that specific product. This policy must include information for consumers regarding the date until which manufacturers will provide security updates.[42]

The end-of-life policy information shall also include information about what consumers can do if they wish to continue using the product in a secure way (e.g. disconnect from the internet). In this context, it is important that consumers are reminded closer to the date that a product is about to be dropped from the security update programme.

Fourthly, it should always be clear whether a proposed update is necessary to improve security, to resolve a software bug, to install new functionalities or whether it serves other purposes. Suppliers must explain the reason of the update and its impact on the product, and importantly, must never misuse the update for example to unilaterally change the conditions of the service. Consumers should be informed about the consequences of not accepting a software update and should not be overloaded with complex technical information.

Furthermore, the update process is often beyond the skill of the average consumer. This is particularly relevant when consumers have to manually download and install the necessary updates. How many consumers know how to update their own router manually? The consequence of this process is usually that products remain insecure and unpatched for several years.[43] Manufacturers must ensure that consumers, including those who are not tech-savvy, can easily install security updates.

Finally, in exceptional circumstances where there is an increased risk to the safety of consumers (e.g. when using a self-driving car), security updates can be installed automatically. However, in this case, the update should only be processed automatically on the condition that (i) consumers are notified about it immediately, (ii) the update does not negatively affect the performance of the connected device and (iii) manufacturers are not circumventing the rules on consent established by data protection legislation, including the ePrivacy Regulation, under the disguise of critical security updates.

**THE RISKS OF NOT UPDATING**

**Health:** in the recent 'Wannacry' ransomware attack, Microsoft issued a patch to correct a vulnerability in their Windows operating system. However, some months later, several companies had not yet implemented the patch therefore remaining vulnerable to a cyberattack. In May 2017, a massive cyberattack exploited this vulnerability and affected more than 200,000 computers worldwide running on Windows by encrypting the users' data and demanding ransom payments. In the United Kingdom, 40 National Health Services (NHS) organisations were affected.

**Financial services:** in 2017, the credit-reporting company Equifax announced that 150 million of people had their personal data (e.g. full names, social security numbers, birth dates) stolen. It was later disclosed that the attack was only possible because Equifax did not patch a critical vulnerability in its software two months before the attack took place.

[42] In this regard, it is important to keep in mind that according to the recently adopted directives on digital content and sales of goods, security updates are part of the conformity definition of a good. Also, consumer sales law remedies are available during the guarantee period, which can be regulated by Member States with a minimum of 2 years.

[43] Bruce Schneier, *Click Here To Kill Everybody*, Norton & Company, 2018, page 37

**BEUC demands:**

- At the time when they are placed on the market, connected products and their associated services must be protected against any known vulnerabilities.
- Security updates should be provided by the manufacturers and service providers during a minimum period of time (depending on the expectations of the consumer and the expected lifespan of the product and its associated service).
- The manufacturers and service providers' end-of-life policy must be clear to the consumers at the time of the purchase. Such policy shall explicitly mention the period until which security updates will be provided.[44]
- Consumers should be informed about the different possibilities once the manufacturer is no longer supporting the product (e.g. disconnect from the internet; dispose it in a responsible way)
- Manufacturers must ensure that consumers, including those who are not tech-savvy, can easily install security updates.
- In exceptional circumstances where there is a safety risk to the consumers (e.g. when using a self-driving car), security updates can be installed automatically provided that certain conditions to protect the consumers autonomy and privacy are met.

### 2.3.2. Strong authentication mechanisms

Lack of or weak ID authentication is often the favourite entrance door for hackers. Our Norwegian member Forbrukerrådet and our UK member Which? discovered that the Bluetooth connection of the I-Que Intelligent Robot, a popular connected toy, was insecure. Because no authentication requirements (e.g. password) were set by default anyone with a smartphone within Bluetooth range could connect to i-Que and use it to start chatting with the child that was playing with the robot.[45]

Connected products and services intended for consumers should by default only accept high-level security authentication methods. For products which use a password, the password must be unique and contain a certain level of complexity and length in accordance to current best practices.

Manufacturers and service providers should be encouraged to add two-factor authentication systems to their default settings. Typically, two-factor authentication systems confirm the users' identity through two different elements: it can be something they know (e.g. password), something they have (e.g. card or personal phone) or something they are (biometrics). Two-factor authentication has been made mandatory (2 of the 3 factors) and successfully implemented in the context of the Payment Services Directive 2 for all electronic payments, in shops or on internet.

It is important to point out that two-factor authentication should only be used for the explicit purpose of securing the connected device. Information provided by the user for the

[44] As mentioned in Chapter 1.1, the Cybersecurity Act will make manufacturers and service providers of *certified* products and services to provide cybersecurity information, including information on the period during which security support (i.e., security updates), to end users.
[45] Connected toys pose child safety risk - Which? Investigates: https://www.youtube.com/watch?v=Ogy7xjEWEpo

purpose of two-factor authentication should not be used for other purposes such as ads or retargeting.[46]

**BEUC demands:**

- Connected products intended for consumers should by default only include high-security authentication features.
- For products and associated services which use a password, the default password must be unique and contain a certain level of complexity and length. If consumers can create their own passwords, those must meet high security features.

### 2.3.3. Encryption

Currently, many connected devices and digital services do not have the most basic encryption[47] protection. Encryption is an essential tool to enhance safety and security in digital products and services. It helps protecting information and is often the last place of defence within a specific product. For instance, even if passwords are breached, encryption systems can prevent hackers from accessing the content of the data.

All manufacturers and service providers should ensure that the data processed in their services as well as the data stored by their connected products is properly encrypted. They should also ensure that third parties that access the data are keeping it properly encrypted in accordance to current best practices.

**BEUC demands:**

- All manufacturers and service providers should ensure that the data stored in their services as well as the data stored by their connected products is properly encrypted in accordance with current best practices.
- The communication between consumer IoT devices, IoT devices and the servers, the manufacturer/service provider and the third parties should be encrypted as well.
- They should also ensure that third parties that access the data are keeping it properly encrypted.

### 2.3.4. Cybersecurity Labels

The Cybersecurity Act stipulates that specific cybersecurity certification schemes can also provide for labels.[48] It is under the responsibility of the Commission based on the work of the EU Cybersecurity Agency (ENISA) and in cooperation with stakeholders and Member States' representatives to decide whether to introduce a label in a particular candidate certification scheme.

In this regard, we would like to underline that the meaning of 'labels' is often unclear and confusing for consumers. CE marking is a good example: many consumers believe that CE marking means that a specific product has been tested to be safe. In reality, for many products, a CE marking is a declaration from the manufacturer, without third party assessment, that the product complies with EU legislation. Similarly, a cybersecurity label

---

[46] Natasha Lomas, *Yes Facebook is using your 2FA phone number to target you with ads*, TechCrunch, 27 September 2018: https://techcrunch.com/2018/09/27/yes-facebook-is-using-your-2fa-phone-number-to-target-you-with-ads/;

[47] Encryption is the process of encoding a message or information in such a way that only authorized parties can access it (definition from Wikipedia)

[48] Article 54 (1) i) of the Cybersecurity Act;

should not give the impression that the product in question is always tested by a third party to be secure.

In the Internet of Things, information for consumers presented in the format of labels about the cybersecurity elements of the products, risk creating confusion to consumers because of the technicality of the subject matter (e.g. information on the encryption system used may not speak to consumers who are not digitally literate). If labels are used to inform consumers, it is important that preliminary qualitative tests are done to ensure that they are well designed and provide the right level of information.

It is important to note that the value of a label also depends on the legal framework in which they are embedded and which should ensure that the appropriate market surveillance mechanisms are in place to check compliance with the label requirements.

In the case of the Cybersecurity Act, national cybersecurity certification authorities have the responsibility to monitor compliance of the manufacturers or providers of ICT with the cybersecurity certification scheme, including compliance of a possible label with the conditions under which it can be used.[49] In this regard, if a label is put in place by a certification scheme, it is important, first, that the conditions under which a label can be used are clearly defined in the certification scheme and are made comprehensible for the average consumer. Second, national cybersecurity certification authorities need to be equipped with the necessary financial and human resources to perform their tasks and ensure compliance of the label with the scheme.

**BEUC demands:**

- Before the establishment of a cybersecurity label under the ENISA certification scheme, the agency should provide for preliminary qualitative testing of such labels to ensure they are well designed and tested for effectiveness, so that end-users correctly understand the meaning of the label.
- If a label is established under a certification scheme, national cybersecurity certification authorities need to be equipped with the necessary financial and human resources to perform their tasks and ensure compliance of the label with the scheme.

### 2.3.5. Isolation of critical systems

Connected products are composed of different layers of software and hardware. Each system plays its part in the functioning of the product. During the design and production process, it is of particular importance to guarantee that for higher risk IoT products, certain critical systems of a connected product are isolated from the rest of the products' systems or internal network. Such measure would prevent serious vulnerabilities to spread from one system to another and thus enhance the resilience of connected products to malicious behaviour.

This principle is particularly discussed in the context of automated and connected vehicles (e.g. a vulnerability in the DVD system should not enable malicious actors to take control of the car).[50]

[49] Articles 54 (1) (i) and 58 (7) b) Cybersecurity Act;
[50] For more information on cybersecurity and connected vehicles, please see page 20

**BEUC demand:**

- During the design and production process, manufacturers should guarantee that the critical systems of certain connected products are isolated from the rest of the products' internal network and thus avoid vulnerabilities to spread from one system to the other.

### 2.3.6. Vulnerability disclosure policy and security oversight

Manufacturers of connected devices and service providers must put in place a vulnerability disclosure policy to reduce the impact of cybersecurity vulnerabilities and data breaches. Bug bounty programs[51] should be considered as an innovative approach to deal with cybersecurity vulnerabilities. It is also important that disclosed vulnerabilities are dealt without undue delay.

**BEUC demands:**

- Manufacturers and service providers must have a 'contact point' through which researchers or users can submit the vulnerabilities they discover.
- Manufacturers and service providers must continuously monitor the security of their products and services.

### 2.3.7. Notification of a cybersecurity breach to the consumers

Another important issue is the notification of a cybersecurity breach to the affected consumers.

Manufacturers and service providers should inform consumers about cybersecurity breaches whenever there is a serious risk that it might affect their personal data (e.g. data breach) or the normal functioning of the product (e.g. vulnerability in a connected vehicle). This notification should also include information on what measures consumers should take to mitigate the effects of the threat.

**BEUC demand:**

- Whenever a security breach may have a serious impact on the interests of consumers, manufacturers and service providers shall inform their users without undue delay and provide them with the necessary information to enable consumers to mitigate the adverse effects of the breach.

### 2.3.8. Cybersecurity and repairability

Today, strict licensing terms imposed by software and device manufacturers prevent consumers from altering their devices according to their needs. This can result in a strange situation where consumers that have paid for a smart product own the physical product but cannot repair the digital content of the product (i.e. the software) if there is a problem or update the software of their devices to ensure their security. This poses problems when the manufacturer and/or service provider decide to end technical support for a product and stop providing security update. What can the consumer do to ensure the product is still protected against cybersecurity risks and vulnerabilities and therefore can continue to use the product safely? In this situation, consumers should be able to undertake all the

[51] Bug bounty program (definition from Wikipedia): a deal offered by many websites, organisations and software developers by which individuals can receive recognition and compensation for reporting bugs, especially those pertaining to exploits and vulnerabilities

necessary measures, such as bringing the device to an independent technical repair service, to keep their products cybersecure.

Another way to expand the security of connected devices is to encourage manufacturers and service providers to make the source code of their software available at the end-of-life. This approach can help to keep otherwise 'obsolete' devices alive through the open source community.

**BEUC demands:**

- Consumers should have a right to repair and modify their products to address security vulnerabilities when the manufacturer is no longer providing security updates.

### 2.3.9. Appropriate response in case of cybersecurity breach

There are situations in which the failure of a connected device or service due to a cybersecurity attack can put in danger the safety of its user and/or of innocent bystanders. What happens if a car is hacked while someone is driving it?[52]

We must ensure that when safety-critical functions of a device are compromised due to a cybersecurity attack, the device responds appropriately and without causing any harm.[53]-[54] For example, for certain appliances (e.g. connected vehicle), consumers can legitimately expect that their smart products disconnect from the internet immediately if experiencing a malfunction.

In the case of a controlled disconnection due to a malfunction it is important that once the internet connectivity is re-established that the devices must re-connect in an orderly fashion, rather than in massive scale to avoid an overload of the system. Also, the lack of connectivity should not prevent the consumer from using the primary function of the device. For example, the lack of connectivity of a smart lock should not prevent someone from opening his door.

**BEUC demand:**

- When safety-critical functions of a device are compromised due to a cybersecurity attack, the device should respond appropriately and without causing any harm.
- If a product or service is forced to unexpectedly disconnect from the internet due to a cybersecurity incident, it must do so in a safe and responsible fashion. The features of a device that in theory does not require connectivity should continue to work when the product or service is not connected to the internet.

[52] Ref.: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
[53] Bruce Schneier, *Click Here To Kill Everybody*, Norton & Company, 2018, p. 109
[54] United Kingdom Department for Transport, *The key principles of vehicle cyber security for connected and automated vehicles*, 6 August 2017, https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles

**CONNECTED AND AUTOMATED VEHICLES**

One of the most important challenges of connected and automated vehicles is cybersecurity. In 2015, two cybersecurity experts famously took over the controls of a Jeep while being driven on the highway. Even though it was for demonstration purposes, this example had the merit of raising awareness and showing how vulnerabilities in connected and automated vehicles can ultimately be life-threatening.

Today, connected and automated vehicles are a junction of connected products, software and systems from different manufacturers and service providers. Unless all different parties – sub-contractors, suppliers and third parties – comply with security by design and by default principles at every stage of the process, it will not be possible to enhance the security of the vehicle.

Particularly important principles for connected and automated vehicles are the necessity to ensure that the security of all software is supported through its lifespan, the encryption of data and the set-up of a system which can react predictably to a cyberattack (e.g. turn-off without causing any harm).

Furthermore, in recent years, several non-critical software systems such as the DVD player or the navigation system were compromised and enabled hackers to gain control of the vehicle. It is therefore of particular important to guarantee that the critical software systems are isolated from the rest of the vehicle's internal network.

In this regard, a systematic threat analysis of the vehicle systems and their environment should be conducted. Manufacturers should also implement a Cyber Security Management System covering the whole life of the vehicle.

## 2.4. Enforcement policy and market surveillance

Under current EU rules, with some exceptions (e.g. medical devices), national authorities in general do not seem to have competence to intervene and for example as ultima ratio withdraw insecure products from the market.

This problem is particularly evident in the context of the current product safety legislation. Traditionally, these laws are interpreted as only being applicable to products whose flaws have an impact on the *physical* safety of consumers. This interpretation is outdated because it excludes devices which can connect to the internet and create new risks for consumers.

As a consequence of such a restrictive approach, market surveillance authorities do not withdraw unsecure connected products from the EU market.

A parallel question is to understand whether products whose security flaws can lead to physical safety concerns fall under the scope of the current product safety rules. Recently, the Icelandic consumer authority introduced a Safety Gate notification in which it

acknowledged that the security vulnerabilities of smart watches for children are a safety problem and thus should be removed from the market under current product safety legislation.[55] In other words, the cybersecurity vulnerabilities of the smart watches were considered as a threat to the safety of its users.

BEUC agrees with the approach from the Icelandic national authorities and encourages other authorities and the European Commission to adopt a similar understanding of current EU product safety rules. On this note, as mentioned in Chapter 1.2, legal certainty would be best achieved via the adoption of a horizontal cybersecurity law.

## 2.5. Standardisation

Standards can be used to embed security requirements at the design phase of the product and to ensure compliance with legal requirements. However, for a standard to be effective, its provisions need to be clear, unambiguous and replicable. This is particularly important in the case of cybersecurity: because security breaches can take multiple forms, objective and measurable requirements are needed to allow for the objective assessment of the security level of connected products.

Furthermore, it is also important to note that while standards can contribute to improve the security of connected devices, standards alone are not the solution as they are a tool of industry self-regulation and not mandatory. Standards dealing with public interest issues should always build on and complement legislation and public policies.

A number of distinct cybersecurity standardisation activities are under way at present. Many of these activities should be seen in the context of the Cybersecurity Act.[56]

### Standard on security requirements of connected products (CEN-CENELEC)

CEN–CENELEC JTC 13 'Cybersecurity and data protection' is aimed at developing a standard for testing the security of consumer connected products. It is based on existing International Consumer Research and Testing[57] (ICRT) methodology about basic security requirements for consumer IoT devices.

Unfortunately, so far, progress has been slow as the group has mainly concentrated on the adoption at the 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)[58]. 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 EU and EFTA, we do not see any of these as containing security product requirements which can increase consumer trust in the connected products they buy. It should also be noted that participating in and influencing the elaboration of international standards requires considerable financial resources, constituting an obstacle for consumer representatives in standardisation bodies. The use of international standards to implement European public policies and legislation is thus our least preferred option.

---

[55] Ref.: https://ec.europa.eu/consumers/consumers_safety/safety_products/rapex/alerts/?event=viewProduct&reference=A12/0157/19&lng=en

[56] According to the Cybersecurity Act, a European cybersecurity certification scheme "*shall include at least the following elements: (...) references to the international, European or national standards applied in the evaluation (...)*".

[57] http://www.international-testing.org/index.html

[58] ISO/IEC 27006, ISO/IEC 27007, ISO/IEC 27010, ISO/IEC 27011, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27019 ISO/IEC 15408-1, ISO/IEC 18045, ISO/IEC 19790, ISO/IEC 30111, ISO/IEC 29147, ISO/IEC 27000.

However, we welcome the recent dialogue between the European Commission and JTC 13 about possible standards to implement future Delegated Acts under the Radio Equipment Directive, in line with our suggestions.

### European Standard for privacy and personal data (CEN-CENELEC)

In 2015, the European Commission requested the elaboration of European standards for privacy and personal data protection management, in support of the Directive 95/46/EC on personal data protection and the Union's security industrial policy. The related work, taking place in WG 5 of CEN–CENELEC JTC 13, is also unfortunately not progressing very fast, with no deliverable published so far. Despite consumer organisations' efforts, the low number of experts and countries participating, and the numerous procedural issues encountered by the group so far make it unlikely any significant result is to be expected.

### Standard on cybersecurity (ETSI)

Cybersecurity standards are also being developed by ETSI TC CYBER, which published one of the first European standards on the subject: ETSI TS 103 645 'Cyber Security for Consumer Internet of Things'. This technical specification for cybersecurity in the Internet of Things, elaborated with our contribution, specifies high-level provisions for the security of internet-connected consumer devices and their associated services.

However, very few of its provisions are of a normative nature, i.e. mandatory to be used for the correct application of the standard; most of the requirements are only recommendations. We believe that more requirements have to become normative in order for the standard to ensure a high level of security. This is what we are advocating for while it is being transposed into a European Norm (EN). In addition, some technical details, such as on vulnerabilities, will need to be added as these are very important and are often neglected by developers and by evaluators.

### Consumer Protection: privacy by design (ISO)

Consumer privacy and security are also at the centre of work at international level in ISO PC 317 'Consumer protection: privacy by design for consumer goods and services', which was proposed by the consumer movement at the European and international level. The aim is to develop a standard ISO 31700 'Consumer protection: Privacy by Design for consumer goods and services', providing high level privacy and security by design lifecycle process requirements. However, specific product requirements will also be needed to complement this horizontal approach, if the standard is to ensure secure products for consumers.

In summary, despite the on-going standardisation activities on security and privacy, both at the European and international levels, there is currently no standard to ensure consumer trust in connected products.

ANEC and BEUC call on the European Commission and the European Standardisation Organisations (ESOs) to step up their efforts to develop European Standards on security of connected products, with the contribution of all concerned stakeholders' expertise. The present parallel approach of CEN-CENELEC and ETSI, reflecting their different membership and decision-making processes, is not conducive to solid results. We therefore recommend a collaborative approach on standards in this area, with an agreement between the ESOs to define which organisation will be responsible for which activities.

In this context, it is important that the standardisation process respects the principles of openness and transparency in its decision-making process, to allow all stakeholders to be able to effectively participate. Consumer participation is essential in ensuring that

standards and conformance systems ensure a high level of consumer protection and counterbalance the industry views, which are the majority

### ANEC and BEUC demands:

- For a standard to be effective, its requirements need to be clear, unambiguous and replicable.
- The European Commission and the European Standardisation Organisations (ESOs) should step up their efforts to develop European Standards on security of connected products, with the contribution of all concerned stakeholders' expertise. The present parallel approach of CEN-CENELEC and ETSI, reflecting their different membership and decision-making processes, is not conducive to solid results. We therefore recommend a collaborative approach on standards in this area, with an agreement between the ESOs to define which organisation will be responsible for which activities.

## 3. Role of the European Network and Information Security Agency (ENISA)

ENISA needs to be a key actor when it comes to increase consumers' trust in the security of connected devices and its related services.

First, as an EU Agency, ENISA needs to promote a more coordinated EU approach towards cybersecurity. In this context, the Agency should actively promote the co-operation between all national enforcement authorities which have to deal with cybersecurity issues. Such a cooperation strategy should include at least the data protection, telecoms and consumer protection authorities.

Also, it is important to ensure a balanced representation between the different ENISA stakeholder groups such as ENISA Advisory Group and Stakeholder Cybersecurity Certification Group. Only one expert out of thirty members of the Advisory Group represents consumers' interests.[59]

Finally, we would like to underline that the ENISA Advisory Group published an opinion on 'Consumers and IoT Security' recently. (The BEUC representative in the Advisory Group was rapporteur of the opinion). Several demands on how ENISA can contribute to improve the security of connected devices can be found there.[60]

### BEUC demands:

- ENISA should pro-actively work towards promoting an EU cybersecurity policy that addresses needs and concerns of and for consumers. This means that the consumers' needs are taken into account regularly and systematically in the relevant cybersecurity policies and that ENISA adapts its work programme to give more space to activities to achieve this objective.

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

- ENISA should actively promote the co-operation between the different national authorities that have to deal with cybersecurity issues. These are at least the data protection, telecoms and consumer protection authorities.
- ENISA should ensure a balance representation between the different stakeholder groups within ENISA's stakeholder bodies.

## 4. Directive on security of network and information systems (NIS Directive)

Recent cyberattacks reconfirmed the need for strong IT security of critical infrastructure. In December 2015, a cyberattack to a power grid left 230,000 Ukrainians in the dark.[61] In June 2019, a cyberattack hit four hospitals in Romania. This attack led to a slowing down of admissions, discharges and prescriptions. The ransomware used to hack the hospitals system would have been detected by antivirus software but none of the affected hospitals had that in place.[62]

The Directive on security of network and information systems obliges Member States to establish a national strategy for the security of network and information systems. This strategy should set out strategic objectives and appropriate policy and regulatory measures. It also obliges Member States to improve the cybersecurity of critical sector operators, including health, energy and financial services, and certain digital service providers such as search engines, cloud services or online marketplaces.

While the NIS Directive is expected to strengthen cybersecurity across the EU, some challenges remain at this stage.

First, the scope of this law is not far-reaching enough, especially when it comes to digital service providers. As recent events have shown us[63] [64], social media platforms are among the digital service providers whose exposure to cybersecurity attacks is among the highest. They have nevertheless been excluded from the scope of the Directive and therefore have no obligation to comply with the NIS cybersecurity rules.

Secondly, the selection procedure of operators of essential services that fall under the scope of the Directive risks creating legal fragmentation in the EU. According to the Directive, it is under the responsibility of each Member State to identify their operators of essential services. Even if the Directive provides a mandatory list of seven key sectors[65], Member States have the autonomy to establish the criteria for the selection of operators of essential services which makes everything more complex and insecure.[66] A recent report from the European Commission reached a similar conclusion.[67]

[61] Ref.: https://www.vice.com/en_us/article/bmvkn4/ukrainian-power-station-hacking-december-2016-report
[62] Ref.: https://www.romania-insider.com/cyberattack-victor-babes-hospital-june-2019
[63] Ref.: https://www.theguardian.com/technology/2018/apr/08/facebook-to-contact-the-87-million-users-affected-by-data-breach
[64] https://www.vice.com/en_us/article/78kk4z/another-day-another-hack-117-million-linkedin-emails-and-password
[65] Annex II – Energy, Transport, Banking, Financial market and infrastructures, health sector, drinking water supply and distribution and digital infrastructure.
[66] For example, in Germany, only companies that reach a threshold of 500.000 customers are identified as an operator of essential services.
[67] Ref.: https://ec.europa.eu/digital-single-market/en/news/report-assessing-consistency-approaches-identification-operators-essential-services

In this context, it must be mentioned that while Member States have a significant level of autonomy to select their operators of essential services, this cannot lead to an exclusion from the scope of the Directive of one of the sectors listed in Annex II.

Another important question is how to ensure the security of key providers who do not fall under the scope of the NIS Directive – e.g. in the health sector, not all hospitals or healthcare professionals may be identified as part of critical infrastructure, and thus will not fall under the scope of the NIS Directive. The above mentioned Wannacry cybersecurity incident affected several private general practitioners in the United Kingdom in 2017.

**BEUC demands:**

- The European Commission must ensure that the implementation of the NIS Directive, in particular the selection of operators of essential services, is consistent all across the EU and that key sectors of society – such as those mentioned in Annex II of the Directive – are not excluded.
- A reform of the NIS Directive must ensure that smaller operators fall under the scope of the Directive. This can be done by an extension of the scope of 'Operators of Essential Services' or by the introduction of a new definition.
- A review of the NIS Directive must include social media platforms in the definition of 'Digital Service Providers'.

### FINANCIAL SERVICES

In the EU, the financial sector has some of the most advanced laws when it comes to the prevention of cybersecurity attacks. In particular, the Payment Services Directive 2 (PSD2) guarantees a high-level of protection for consumers. It establishes strong customer authentication requirements and it also forces payment service providers to immediately inform consumers if any problem arises with regard to their bank account.

Despite this, consumers still face significant setbacks when financial organisations are part of a cybersecurity incident.

Considered to be the first digital heist of the payment sector, the Tesco Attack is a good example of what can go wrong for the consumers in the case of a cyberattack to a financial organisation. During the weekend of 6-7 November 2016, about 9,000 current accounts were relieved of between twenty and several hundred pounds sterling (270 on average). The total damage was estimated at 2.5 million pounds. Part of the online services were closed, preventively, and a renewal of the cards of the targeted people was initiated.

On Monday morning, the bank issued a general alert, reporting a cyberattack (without further details) targeting more than 40,000 accounts in total. In practice, it means that 40,000 cardholders were unable to use their cards during several days and had no access to their account.

These events lead to several questions but most importantly how to ensure that consumers are compensated for the inconvenience resulting from the inability to use a personal payment card for a certain period of time? Unfortunately, when it comes to the definition of 'additional compensation', the PSD2 remains vague and does not provide an appropriate solution.

## 5. Cybersecurity incident reporting

Several EU laws have established incident reporting requirements in case of a cyberattack. For example, Articles 33 and 34 of the GDPR, Article 96 of the Payment Services Directive 2 (PSD2), Articles 6, 14 and 16 NIS Directive.

Unfortunately, these rules lack consistency in at least two key points: the time frame in which the companies have to report the cybersecurity incident to the European or national relevant authority and the approach towards consumer notification.[68]

Regarding the time frame issue, the NIS Directive refers to 'without undue delay' and the GDPR establishes a deadline of 72h in case of a data breach.

As for the second element, while these three laws refer to the notification to the consumer in case of a cybersecurity attack, each one has its own specific requirements. For example, the GDPR requires a notification to the consumer in case of a data breach only when it is likely to result in a high risk to the rights and freedoms of the affected consumers. The PSD2 mentions the notification to the consumer when the incident is likely to have an impact on the financial interests. Finally, the NIS Directive enables the competent authority to notify the consumer when the incident is in the public interest.

This fragmentation in the case of an incident reporting leads to uncertainty and lack of efficiency[69]. For example, in the case of data breach in the financial services sector, which rules and procedures should the financial institution comply with when it comes to communicating the incident to the consumers? Those of the GDPR, NIS Directive (if financial institution were identified by the relevant Member State as an operator of essential service) or PSD2? Will this result in less consumers being notified of a cybersecurity incident?

**BEUC demand:**

- The European Commission shall put in place a common cybersecurity incident reporting system that ensures a timely notification to the consumers in all circumstances.

END

[68] Ref.: https://www.ceps.eu/ceps-publications/cybersecurity-finance-getting-policy-mix-right/
[69] Ref.: https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

*This publication is part of an activity which has received funding under an operating grant from the European Union's Consumer Programme (2014-2020).*