orgalim
EUROPE'S TECHNOLOGY INDUSTRIES

POLICY PAPER

Brussels, 9 November 2020

Proposal for a horizontal legislation on cybersecurity for networkable products within the New Legislative Framework[1]

Executive summary

Cybersecurity is a wide-ranging issue which touches on almost every aspect of life and affects a multitude of industrial areas. It is an essential precondition for all networkable products and crucial for the continued growth of Europe's economy and its society.

Currently, various legislative reviews are under way or planned, which might further impact the way cybersecurity is being addressed in the EU. Many of these concerns are directly related to tangible products communicating over the internet ('networkable products') which are offered by Europe's technology industries. Despite the fact that the above-mentioned legal initiatives may address valid cybersecurity concerns, if implemented as they stand, they will clearly lead to **regulatory fragmentation** with overlapping and contradicting requirements for manufacturers. Orgalim is convinced that, specifically for networkable products, a coherent regulatory framework is of the utmost importance, especially in the context of the Single Market. Therefore, Orgalim proposes the introduction of a **horizontal legislation on cybersecurity for networkable products within the New Legislative Framework** (NLF). The key elements (scope, essential requirements for networkable products, obligations to economic operators, conformity assessment, reference to standards and market surveillance) of such legislation can be found below in this document.

Orgalim is convinced **that drawing up a single horizontal legislation on cybersecurity for networkable products within the NLF would be the best policy option to protect Europe against cybersecurity risks while strengthening the EU's Single Market**. If all actors are working together, the implementation of this option would be achieved more quickly than by drawing up individual fragmented regulations as is currently envisioned by the legislators.

[1] New Legislative Framework (NLF), as laid out by Decision 768/2008, in conjunction with Regulation 765/2008 and Regulation 2019/1020 (Market Surveillance), Regulation 1025/2012 (standardization)

1. INTRODUCTION

Cybersecurity is a wide-ranging issue which touches on almost every aspect of life and affects a multitude of industrial areas. It is an essential precondition for all networkable products and crucial for the continued growth of Europe's economy and its society. In representing Europe's technology industries, we recognise its importance and horizontal nature as well as the ambition shared by businesses, consumers and citizens to enhance the EU's cybersecurity capabilities.

The EU's cybersecurity policy has been developed in response to three drivers: preserving the Single Market, combating terrorism, and playing a global role. It started in 2013 when a fully-fledged EU Cybersecurity Strategy was launched, and a landmark of EU cybersecurity law focused on economic resilience was proposed: the Network and Information Security Directive (NIS Directive)[2]. In 2017, several additional legislative proposals were introduced:

- the EU Cybersecurity Act, which introduced EU-wide IT security certification and an extended mandate for the cybersecurity agency ENISA. However, the EU Cybersecurity Act is not directly applicable to the extension of the Single Market for (digital) products, in particular networkable products,
- legislation for a common approach to the scrutiny of foreign direct investment including for cybersecurity concerns,
- and legislation for strengthening EU cybersecurity competence.

2. THE CHALLENGE: FRAGMENTATION

Currently, various legislative reviews are under way or planned, which might further impact the way cybersecurity is being addressed in the EU. Examples of such initiatives aiming to address cybersecurity concerns, through legislation or in other ways, are:

- The review of the Directive on Security of Network Information Systems (the NIS Directive)
- The review of the Machinery Directive (MD)
- The review of the General Product Safety Directive (GPSD)
- Delegated Acts under the Radio Equipment Directive (RED)
- Several certification schemes under the Cybersecurity Act (CSA)
- National initiatives, such as the so-called German IT Security Law 2.0.

Many of these concerns are directly related to tangible products communicating over the internet ('networkable products') which are offered by Europe's technology industries. Despite the fact that the above-mentioned legal initiatives may address valid cybersecurity concerns, if implemented as they stand, they will clearly lead to **regulatory fragmentation** with overlapping and contradicting requirements for manufacturers. This approach will impact the Single Market, with respect to the free movement of goods. It could also weaken the competitiveness of European manufacturers in the global market, where we would deviate from international cybersecurity practices.

In 2019, Orgalim put forward seven principles of "Good Cybersecurity Policy". These principles should serve as guidance to preserve the benefits of the Single Market, and to ensure the necessary level of cybersecurity in the EU.

We would like to specifically emphasise the first three key principles, as they are especially relevant in the context of a possible fragmentated approach:

[2] Directive (EU) 2016/1148 concerning measures of a high common level of security of network and information systems across the Union.

- A European approach to cybersecurity:
  to ensure a harmonised framework at EU level with the aim of building a real single market for cybersecurity.
- Consistent and coherent legal requirements:
  to avoid patchy, overlapping and inconsistent cybersecurity requirements in European legislation.
- Common cybersecurity goals to ensure horizontal consistency:
  applying to the products, solutions, and processes.

Orgalim is convinced that, specifically for networkable products, a coherent regulatory framework is of the utmost importance, especially in the context of the Single Market. We need to avoid contradictory requirements by different laws for the same products, as these create technical impossibilities. This can be the case at the European level, or because of potential conflicting requirements between Member States. These can all create critical barriers for the free movement of goods in the EU.

When it comes to creating coherence and harmonising the EU legislation on products (including the networkable products), the New Legislative Framework (NLF) is the proven cornerstone. Such legislation follows the model provisions of Decision 768/2008.

However, to gain the most benefit from the harmonising effect of the NLF, we believe that cybersecurity needs to be addressed through a single horizontal cybersecurity legislation within the context of the NLF framework. This is the only way in which fragmentation can be avoided from the outset, even within the NLF. Such new legislation, if done correctly, will ensure a stronger coherence across the EU, and will provide clarity for manufacturers of networkable products on how cybersecurity measures will be applied in the future.

Therefore, Orgalim proposes the introduction of a **horizontal legislation on cybersecurity for networkable products within the New Legislative Framework** (NLF). The key elements of such legislation can be found below in the next chapters of this document.

3. THE SOLUTION: A HORIZONTAL LEGISLATION ON CYBERSECURITY FOR NETWORKABLE PRODUCTS WITHIN THE NLF AND ITS ADVANTAGES

A horizontal legislation on cybersecurity for networkable products within the NLF would provide the following advantages, most of them well-known from the NLF legislation:

- Full coherence and no risk of contradictions due to only one legislative reference for both manufacturers and enforcement authorities.
- Building on the continuous updating process of harmonised standards to reflect the state of the art in cybersecurity.
- Flexibility in conformity assessment due to several well established assessment procedures, including self-declaration.
- Free movement of goods adhering to the same common rules on cybersecurity within the European Single Market.
- Existing network of market surveillance authorities.

The European Commission is currently pursuing the idea of proposing Delegated Acts – under the Radio Equipment Directive amongst others – on privacy and fraud. Orgalim would like to point out that the above-mentioned approach would be more transparent and effective in addressing the challenges of cybersecurity, because it has the following advantages over the Delegated Acts:

- It directly addresses cybersecurity instead of regulating privacy, data protection and protection against fraud – all of which are already covered by other regulations.
- It will cover ***all*** types of networkable products (including non wireless ones).
- Unlike Delegated Acts, a horizontal legislation on cybersecurity for networkable products provides a more inclusive way of law-making. It ensures transparency in the law-making process and the opportunity for all relevant stakeholders to participate in it.

4. DETAILS OF THE PROPOSAL FOR A HORIZONTAL LEGISLATION WITHIN THE NEW LEGISLATIVE FRAMEWORK (NLF)

We would like to propose the following key elements of such a horizontal legislation on cybersecurity for networkable products within the NLF.

4.1. Scope

The legislation should address '**Networkable Products**'. These are:

a. Products intended for communication over the internet by using any internet protocol

b. Products for which communication over the internet by using any internet protocol is reasonably foreseeable, irrespective of their intended use

Networkable products also include the associated embedded firmware and software that is essential for the primary function of the end product and is either:

c. pre-installed on a product in accordance with a or b, or

d. separately placed on the market by the hardware manufacturer or a software manufacturer and downloaded to a product at a later stage in accordance with a and b, for example in the form of an extension to functionality

Note: In the industrial context, the term 'product' also includes 'components' and 'systems'.

4.2. Essential Requirements for Networkable Products

The "Blue Guide on the implementation of EU product rules"[3] states that "Union harmonisation legislation limits legislative harmonisation to a number of essential requirements that are of public interest. Essential requirements define the results to be attained, or the hazards to be dealt with, but do not specify the technical solutions for doing so". This is also applicable to cybersecurity. The respective "Essential Requirements" must address which risks of cybersecurity are to be mitigated, whereas technical details and further domain-specific specifications are left to harmonised standards listed in the Official Journal of the EU.

[3] Official Journal of the European Union, C272/1, 26.7.2016

4.3. Obligations to economic operators

The NLF names and defines several economic operators. For Orgalim it is of the highest importance that the horizontal legislation clarifies obligations to manufacturers[4] as well as the limits of such obligations.

The key obligation for a manufacturer: ensure that networkable products are designed and manufactured so that they are suitable for their intended use, and in the respective operational environment conform to the above-mentioned essential requirements at the time of placing them on the market, taking into account the known risk and state of the art with respect to cybersecurity.

The very important question of addressing cybersecurity beyond the placing on the market can be handled as an explicit obligation, for instance by disclosure at the time of placing on the market the timeframe and the scope of the support for cybersecurity of the networkable product. However, it would also be possible to address this via above-mentioned standards.

Further obligations for manufacturers can be set up, similarly to current NLF legislation. For the sake of clarity we do not elaborate on them here.

The resilience of a networkable product to cyberattacks after its placing on the market is the responsibility of various stakeholders (e.g. manufacturers, end users etc.) so it might be reasonable to stipulate cybersecurity obligations for economic operators other than manufacturers. This can be done in the same horizontal legislation on cybersecurity for networkable products or other legislations, e.g. occupational health and safety legislation relevant for plant operators.

Note: Integrators (see ISO 11161) are manufacturers. If integrators use networkable products already assessed for conformity according to this legislation, the obligations and procedures may be reduced. Nevertheless, integration solutions (for example the composition and interconnection of products to a final product) are also subject to the regulation and thus the cybersecurity of the final product is covered by the NLF.

4.4. Conformity Assessment

Well established procedures for conformity assessment of the essential requirements are another strength of the NLF. The framework offers several procedures for conformity assessment (so called modules in Decision 768/2008). These procedures range from what is known as self-assessment or self-declaration (Module A, Internal Production Control in above-mentioned Decision) up to full quality assurance including the third party design examination.

Many of the products bearing a CE mark are currently undergoing the Module A conformity assessment. The advantage of this assessment is a shorter time to market and higher flexibility for innovative products. This advantage should also be retained for cybersecurity because it is a key feature, especially in rapidly moving and highly innovative market segments.

Depending on the intended use, different conformity assessment procedures may be foreseen.

Within the conformity assessment the assessment of the risk associated with the networkable product is a key concept. The measures to meet the "Essential Requirements" are risk dependent, with risk considered as the combination of impact and probability under the conditions of the product's intended use[5]. This concept is directly applicable to cybersecurity.

[4] See Annex for definition

[5] This approach is well covered in risk assessment procedures (e.g. ISO 12100)

4.5. Reference to Standards

As usual in the new approach or the NLF, harmonised standards on cybersecurity for the concerned networkable product groups would define technical details. Once their references are published in the Official Journal of the EU and listed under the respective harmonised legislation, their use would grant the manufacturer presumption of conformity to the legislation. Reference to standards makes the legislation more flexible, for instance to reflect changes in the state of the art which is extremely relevant for cybersecurity with its inherent challenges of the rapid development of both potential attacks and protection measures.

It is well known that several cybersecurity standards exist[6] or are in the process of being developed. Certainly, further improved or new standards would be introduced by the European Standardisation Organisations to meet the future standardisation requests that are expected under a horizontal legislation on cybersecurity for networkable products.

4.6. Market Surveillance

Any legal requirement needs effective enforcement. Legislation under the NLF can build on a long history of effective market surveillance that has recently been further strengthened through Regulation (EU) 2019/1020.

5. CONCLUSIONS

Orgalim is convinced that drawing up a single horizontal legislation on cybersecurity for networkable products within the NLF would be the best policy option to protect Europe against cybersecurity risks while strengthening the EU's Single Market. If all actors are working together, the implementation of this option would be achieved more quickly than by drawing up individual fragmented regulations as is currently envisioned by the legislators. **Orgalim, its member associations and all their member companies stand ready to support the EU legislators in the implementation of the proposed approach on cybersecurity, which could contribute to a safer and more prosperous Europe.**

[6] E.g. IEC 62443 4-2, ETSI EN 303645, ISO 27000 series

Orgalim represents Europe's technology industries, comprised of 770,000 innovative companies spanning the mechanical engineering, electrical engineering, electronics, ICT and metal technology branches. Together they represent the EU's largest manufacturing sector, generating annual turnover of over €2,100 billion, manufacturing one-third of all European exports and providing 11.5 million direct jobs. Orgalim is registered under the European Union Transparency Register – ID number: 20210641335-88.

6. ANNEX – DEFINITIONS

***Cybersecurity*[7]:**

Encompasses all measures and capabilities of a product (hardware and software) for assurance of confidentiality, availability and integrity based on its intended use.

***Placing on the market*[8]:**

The first making available of a product on the Union market.

***Manufacturer*[9]:**

Any natural or legal person who manufactures a product or has a product designed or manufactured, and markets that product under his name or trademark.

***Harmonised Standard*[10]:**

Means a European standard adopted on the basis of a request made by the Commission for the application of Union harmonisation legislation.

'European standard' means a standard adopted by a European standardisation organisation.

***Conformity Assessment*[11]:**

The process demonstrating whether specified requirements relating to a product, process, service, system, person or body have been fulfilled.

***Market surveillance*[12]:**

The activities carried out and measures taken by market surveillance authorities to ensure that products comply with the requirements set out in the applicable Union harmonisation legislation and to ensure protection of the public interest covered by that legislation.

***End user*[13]:**

Means any natural or legal person residing or established in the Union, to whom a product has been made available either as a consumer outside of any trade, business, craft or profession or as a professional end user in the course of its industrial or professional activities.

***Intended use*[14]:**

Means the use of a product in accordance with the information provided in the instructions for use.

***Operational environment*[15]:**

Means the environment in which the product is used as intended, as defined in the instructions for use. The 'intended use' and the 'operational environment' are intertwined.

[7] There is no unique definition. Text based on definitions in standard ISO/IEC 27032 and Regulation (EU) 2019/881
[8] Original Text from Decision 768/2008/EC Article R1.3, updated in Regulation (EU) 2019/1020, Art 3(2)
[9] Decision 768/2008/EC, Article R1.3
[10] Regulation (EU) 1025/2012, Article 2(1)
[11] Decision 768/2008/EC, Article R1.12
[12] Regulation (EU) 2019/1020, Art 3(3)
[13] Regulation (EU) 2019/1020, Art 3(21)
[14] Based on Directive 2006/42/EC, with machinery exchanged by product
[15] Based on IEC 62443 series