Proposal COM(2022) 454 of 15 September 2022 for a **Regulation on horizontal cybersecurity requirements for products with digital elements** and amending Regulation (EU) 2019/1020.

CYBER RESILIENCE ACT

cepPolicyBrief No. 1/2023

LONG VERSION

Author: Dr Anastasia Kotovskaia, LL.M. | kotovskaia@cep.eu
cep | Schiffbauerdamm 40 | 10117 Berlin | Phone 030-43973746-13 | www.cep.eu

A. Key elements of the EU proposal

1 Context and objectives

- According to the Commission, software and hardware products have been increasingly affected by cyberattacks in recent years. A major reason for this is a low level of cyber security of these products, which often have vulnerabilities that are inadequately or belatedly closed. [p. 1]
- In 2021 alone, cybercrime caused damage amounting to 5.5 trillion € worldwide. Successful cyberattacks resulting from a lack of cybersecurity of software and hardware products include the Ramsonware worm "WannaCry", which exploited a vulnerability in "Windows", and the Kaseya VSA attack, in which a network management software from Kaseya showed security vulnerabilities. [p. 1]
- Cybersecurity incidents involving products with digital elements can impact organisations and supply chains, spread rapidly across the single market and lead to "significant societal and economic costs". However, most hardware and software products do not yet have EU legislation targeting their cybersecurity. [p. 1]
- The Commission has therefore presented a proposal for a Cyber Resilience Act (CRA). The CRA establishes a legal framework for the development and placing on the market of cyber-secure products with digital elements (hereafter "pwde") in the EU. [p. 1]
- The CRA specifically establishes [Art. 1]
  - requirements for the design, development, manufacture and placing on the market of pwde,
  - obligations for relevant economic operators, i.e. manufacturers, importers and distributors,
  - requirements for dealing with vulnerabilities, and
  - specifications for monitoring the market for pwde and enforcing the requirements of the CRA.
- The Commission's aim is. in particular, to [pp. 1 and 8, Recitals 1, 2 and 4].
  - establish uniform cybersecurity requirements for manufacturers, importers and distributors of pwde,
  - ensure that pwde manufacturers improve the cybersecurity of their products at the design and development stage so that they come to market with fewer vulnerabilities,
  - ensure that manufacturers take any cybersecurity risks during the product lifecycle seriously,
  - strengthen transparency about the security features of pwde so that product users can better assess the cybersecurity features of a product when making a purchasing decision,
  - reduce the number of cyber security incidents and associated costs and reputational damage for manufacturers, importers and distributors of pwde, and
  - strengthen the attractiveness of pwde from the EU.

2 Scope of application

- The CRA applies to all "products with digital elements (pwde)". "Pwde" are "connectable" software products or hardware products whose use involves a data connection to a device or network. Software and hardware components that are to be placed on the market separately ("non-embedded") are also considered "pwde". In addition, "pwde" also include any "remote data processing solutions" of the software and hardware products without which the pwde could not perform any of its functions. [Recital 10, Art. 2 (1), Art. 3 (1), (2) and (6-12)]
- The CRA does not apply to pwde provided that they are [Art. 2 (2)]
  - medical devices or in vitro diagnostic medical devices for human use, and
  - motor vehicles, as well as systems, components and technical units of these vehicles.

  Sector-specific cybersecurity rules already exist for these [Recitals 12 and 13].
- The CRA also does not apply to pwde provided that they are [Recital 10, Art. 2 (3) and (5)].
  - aeronautical products, parts and appliances and have already been certified with regard to safety requirements under the Civil Aviation Regulation (EU) 2018/1139,
  - developed exclusively for national security or military purposes,
  - specifically serve the processing of classified information, or
  - are free and open source software products that are developed or provided outside of a commercial activity.

- The application of the CRA may be restricted or excluded if other EU regulations contain rules that are comparable to the essential requirements of the CRA. This applies only if [Art. 2 (4)]:
  - the restriction or exclusion is compatible with the existing regulations applying for this pwde,
  - the sector-specific regulations guarantee the same level of protection as the proposed CRA.

  The Commission may adopt delegated acts to this effect.

3 Products with digital elements - classification into four groups

- Pwde are basically divided into four groups, depending on their degree of risk [Art. 6 (1) and (5), Recitals 26, 27 and 62]:
  - Non-critical pwde: These are pwde that do not fall under any of the other groups. These include hard disks, word processing software and PC games.
  - Critical pwde (Class I): These include, among others, browsers and password managers.
  - Critical pwde (Class II): These include operating systems for servers, desktops and mobile phones, public key infrastructures, firewalls for industrial use, routers, security elements and smart cards.
  - Highly critical pwde: No pwde fall under this group yet.

  Approximately 90% of the market should fall into the group of non-critical pwde. No more than 10% of the market should be considered critical [Impact Assessment part 1/3, p. 48].

- The Commission may, by means of delegated acts, add new categories of critical products to the lists of critical pwde – class I and II – or remove individual categories from these lists. In doing so, it shall take into account the level of cybersecurity risk of the respective product category and shall make its decision on the basis of the following criteria [Art. 6 (2)]:
  - cybersecurity-related functionality of the pwde,
  - use of the pwde in sensitive environments, e.g. in industrial environments or by "essential" facilities – e.g. energy suppliers, airports, operators of internet nodes – as defined in the NIS 2 Directive (see **cepAdhoc**),
  - extent of any loss or disruption already caused by the use of a pwde, and
  - cause for significant concern that adverse impacts could arise from the use of a pwde.

- The Commission may, by means of delegated acts, establish a list of categories of highly critical pwde. In doing so, it shall examine in particular whether a product category [Art. 6 (5)]
  - meets one or more of the criteria for determining class 1 and class 2 critical pwde,
  - is used by, or is potentially significant for the activities of, essential facilities within the meaning of the NIS 2 Directive, or
  - is relevant to the resilience of the pwde supply chain.

4 Security requirements for products with digital elements

- Pwde shall, inter alia, [Annex I, Part 1, Section 1]
  - be designed, developed and manufactured in such a way as to ensure an appropriate level of cyber security,
  - be delivered without known exploitable vulnerabilities,
  - be provided in a secure standard configuration,
  - offer the possibility to reset the product to its default configuration,
  - contain appropriate control mechanisms against unauthorised access,
  - ensure the confidentiality and integrity of personal and other data,
  - respect the principle of "data minimisation"; data processing must therefore be limited to what is necessary for the intended use of the product, and
  - ensure that security updates are available to address vulnerabilities.

5 Requirements for dealing with vulnerabilities

- A "vulnerability" is the weakness, susceptibility or malfunction of an ICT product or service that can be exploited in the event of a cyber threat [Art. 3 (39) in conjunction with Art. 6 (15) NIS 2 Directive].

- Manufacturers of pwde shall, inter alia, [Annex I, Part 1, Section 2].
  - identify and document vulnerabilities and components of the product, for example in a "Software Bill Of Materials" (SBOM), i.e. a record of the components included in the software elements of a pwde,
  - address and rectify vulnerabilities "without delay",

- ensure that security patches and updates are provided "without delay" and "free of charge" as soon as they are available,
- regularly test the safety of their pwde,
- publicly disclose information about fixed vulnerabilities as soon as they have provided security updates,
- take measures to facilitate the exchange of information about potential vulnerabilities in their product with third parties.

6 Obligations of economic operators

The CRA establishes horizontal requirements for all economic operators in the value network of a pwde, i.e., in particular, the manufacturers, importers and distributors [Chapter II, Art. 3 (1) Nr. 17].

6.1 Obligations of the manufacturers

- Before placing pwde on the market, manufacturers must, in particular,
  - ensure that they comply with the security requirements (see section 4) [Art. 10 para. 1],
  - assess the cybersecurity risks associated with the product [Art. 10 (2)],
  - take account of the findings of the evaluation in the planning, design, development, manufacture, supply and maintenance of the product [Art. 10 (2)],
  - prepare a technical documentation (see section 7 for more details) [Art. 10 (7)], and
  - carry out conformity assessment procedures or have them carried out (for more details see section 7) [Art. 10 (7)].
- Manufacturers of pwde must also, in particular,
  - systematically document relevant aspects concerning the cyber security of its product, including vulnerabilities of which they become aware [Art. 10 (5)],
  - provide for remediation of vulnerabilities; this applies to [Art. 10 (6)], whichever is shorter
    - the expected lifetime of the product, or
    - five years from the date on which the product is placed on the market,
  - have policies and procedures in place to address vulnerabilities reported to them, including vulnerability disclosure policies [Art. 10 (6)], and
  - "immediately" – for the expected lifetime of the product or five years from the date of placing the product on the market, whichever is shorter - take corrective action if they know or have reason to believe that their pwde does not comply with the security requirements (Section 4) or the vulnerability management requirements (Section 5); this may include the recall or withdrawal of the product [Art. 10 (12)].
- Manufacturers of pwde must provide information and guidance to product users, including [Art. 10 (10), Annex 2]:
  - the contact details of the manufacturer,
  - the contact to which information about vulnerabilities can be reported,
  - on the intended use of the product and its key functions,
  - information under which circumstances cyber security risks could occur when using the product,
  - on technical support, including information on how long the user can expect security updates,
  - how to safely commission the product for the first time, to install safety updates, and to safely decommission the product.
- Pwde manufacturers must also report any cybersecurity incident affecting their pwde and any actively exploited vulnerability to the European Union Cyber Security Agency (ENISA) within 24 hours. The notification must include information on the incident or vulnerability. [Art. 11 (1) and (2)] Notifications of massive cybersecurity incidents and crises at operational level must be forwarded by ENISA to the European Network of Cyber Crisis Liaison Organisations (EU-CyCLONe) [Art. 11 (3)].
- Manufacturers of pwde must also inform users of Pwde about cybersecurity incidents and, if necessary, inform them what measures they can take to limit the consequences of an incident [Art. 11 (4)]. Manufacturers can either contact their customers directly or publish a notification on their website [Recital 35].
- Pwde manufacturers must report vulnerabilities in a component that is integrated into their pwde to the person or entity maintaining the component [Art. 11 (7)].

6.2 Obligations of importers and distributors

- Importers may only place pwde on the market if they meet the security requirements (see section 4) and the requirements for dealing with vulnerabilities (section 5) [Art. 13 (1)]. To do this, they must check whether the manufacturer's pwde has undergone a conformity assessment procedure, whether technical documentation is available and whether the product bears the CE marking [Art. 13 (2)].
- Distributors must take "due care" when placing a pwde on the market to ensure that the requirements of the CRA are met. Among other things, they must check that the product bears the CE marking and that the manufacturer's information and instructions concerning the product are available. [Art. 14 (1) and (2)]
- If an importer or distributor finds that the requirements are not met, they may not place the pwde on the market until the requirements are met [Art. 13 (3), Art. 14 (3)]. If they find that a pwde does not comply with the requirements after it has been placed on the market, they shall immediately ensure that the necessary corrective measures are taken or, if necessary, withdraw the product concerned from the market or recall it [Art. 13 (6), Art. 14 (4)].
- Where there is a significant cyber security risk, importers and distributors must inform the manufacturer and market surveillance authorities [Art. 13 (3) and (6), Art. 14 (3)].
- Importers must ensure that the pwde is accompanied by the manufacturer's information and instructions on the product [Art. 13 (5)].
- Importers and distributors must provide the market surveillance authorities, upon their request, with all information demonstrating the conformity of the pwde with the requirements [Art. 13 (8), Art. 14 (5)].

7 Conformity assessment procedure

A "conformity assessment" verifies whether a pwde meets the security requirements (section 4) and the requirements for dealing with vulnerabilities (section 5) [Art. 1 (28)].

7.1 Presumption of conformity

- For pwde, compliance with the cybersecurity requirements is "presumed" if
  - they comply with harmonised EU standards or parts thereof [Art. 18 (1)].
  - they comply with "common specifications" adopted by the Commission by means of implementing acts; this applies if there are no or insufficient harmonised EU standards for the pwde [Art. 18 (2) and Art. 19], or
  - for which an EU declaration of conformity or certificate has been issued under an EU cybersecurity certification scheme pursuant to Regulation (EU) 2019/881 (see **cepPolicyBrief**) [Art. 18 (3)].
- The Commission may, by means of implementing acts, specify, inter alia, the EU cybersecurity certification schemes that may be used to demonstrate the compliance of a pwde [Art. 18 (4)].

7.2 Conformity assessment

- Conformity assessment procedures will be established. These are intended to verify compliance with product and process-related requirements throughout the lifecycle of pwde. Modules for such procedures will be used, based on the risk and the level of safety required. [Recital 44]
- Manufacturers of Pwde can use three possible procedures for conformity assessment [Art. 24 (1) in connection with Annex VI and Decision No. 768/2008/EC]:
  1. internal control procedures (module A),
  2. EU type-examination procedures (module B) followed by the procedure based on internal production control (module C), or
  3. full quality assurance (module H).
- Manufacturers of non-critical pwde (Group 1) can check the conformity of their product by "self-assessment" according to the procedure based on module A. They may also choose, on a voluntary basis, a more stringent conformity assessment procedure. [Recital 45]

- Manufacturers of critical pwde of class 1 (group 2) must assess the conformity of their product according to the procedures based on modules B and C or module H. If harmonised EU standards, common specifications or EU certification schemes exist, they may also use them for conformity assessment. [Art. 24 (2)]
- Manufacturers of critical pwde of class 2 (group 3) must assess the conformity of their product according to the procedures based on modules B and C or module H [Art. 24 (3)]. The conformity assessment must always be carried out by a third party [Recital 45].
- Manufacturers of highly critical pwde (group 4) must demonstrate the conformity of their product by obtaining a European cybersecurity certificate under an EU certification scheme [Art. 6 (5)].
- Manufacturers of pwde must issue an EU declaration of conformity. This must be continuously updated and certify compliance with the requirements [Art. 20 (1)].

7.3 Technical documentation and CE marking

- Before placing their pwde on the market, manufacturers must prepare a "technical documentation" [Art. 10 (7) in conjunction with Annex V]. This must contain information on the means used by the manufacturer to meet the essential requirements [Art. 23 (1)]. The technical documentation must be continuously updated during the expected lifetime of the product or a period of five years after the product has been placed on the market, whichever is shorter [Art. 23 (2)].
- Manufacturers must affix the "CE marking" to their pwde before placing it on the market [Art. 10 (7), Art. 22]. With this, the manufacturer signals that the product meets the security requirements (section 4) and the requirements for dealing with vulnerabilities (section 5) [Art. 2 (32)].

8 Market surveillance and enforcement

8.1 Role and powers of the market surveillance authorities and the Commission

- Each Member State shall designate one or more market surveillance authorities [Art. 41 (2)].
- If a market surveillance authority of a Member State considers that a pwde poses a "significant cybersecurity risk", it may carry out an assessment of the product. If it concludes that the product does not comply with the requirements of the CRA, it shall "without delay" require the relevant market actor to take appropriate corrective action, to withdraw the product from the market or to recall it. [Art. 43 (1)]
- If the risk does not only affect the territory of the market surveillance authority, the latter must inform the Commission and the other Member States about the assessment and the corrective measures taken [Art. 43 (2)].
- If the manufacturer of a pwde does not take appropriate corrective action within the set time limit, the market surveillance authority must take appropriate "interim" measures. This includes prohibiting or restricting the making available of the product on its national market. The authority must also inform the Commission and the other Member States. [Art. 43 (4)]
- If there are no objections to a provisional measure from a Member State or the Commission within three months of its initiation, the measure is deemed justified. The market surveillance authorities of all Member States shall then ensure that appropriate restrictive measures are taken "without delay" in respect of the product concerned. [Art. 43 (7) and (8)]
- If, on the other hand, there are objections to a provisional measure, the Commission investigates the provisional measure and must decide within nine months whether it is justified or not. If it is justified, all Member States must ensure that the non-compliant pwde is withdrawn from the market. If it is not justified, the Member State must withdraw its corrective measures. [Art. 44 (1) and (2)]
- If the Commission is satisfied that a pwde posing a significant cybersecurity risk does not comply with the CRA, it may request a competent market surveillance authority to carry out an assessment of the product [Art. 45 (1)].
- In exceptional cases, such as where the relevant market surveillance authorities have not decided on corrective measures, the Commission may also instruct ENISA to carry out an investigation. Based on the results of this investigation, the Commission may decide on corrective measures, including ordering the withdrawal or

recall of the product concerned within a reasonable period of time. It shall take such a decision by means of an implementing act. [Art. 45 (2-4)]

- Market surveillance authorities may carry out "sweeps", i.e. coordinated checks to determine whether certain pwde, which often present cybersecurity risks, comply with the requirements of the CRA. They are usually coordinated by the Commission. ENISA identifies categories of pwde for which a sweep should be organised. [Art. 49]

8.2 Sanctions for non-compliance with the requirements of the CRA

- Member States must lay down rules on penalties applicable to infringements of the requirements by economic actors. The sanctions must be "effective, proportionate and dissuasive". [Art. 53 (1)]
- For violations of the security requirements (Section 4), the vulnerability management requirements (Section 5) and the manufacturer-related obligations, administrative fines apply up to [Art. 53 (3)]
  - 15 million € or
  - 2.5% of the company's total worldwide annual turnover in the last financial year,

  whichever is higher.
- For other violations, administrative fines apply of up to
  - 10 million € or
  - 2% total worldwide annual turnover of the company in the last business year,

  whichever is higher.

9 Interaction between the CRA and other EU legal acts

- The CRA specifically regulates the handling of cyber security risks. However, pwde may also pose other safety risks. These other risks will continue to be covered by the General Product Safety Regulation, which is intended to replace the existing Product Safety Directive 2001/95/EC soon. [Recital 28, Art. 7]
- Pwde that are classified as high-risk AI systems under the proposed AI Regulation [AI Regulation, COM(2021) 206, s. **cepPolicyBrief**] must comply with the cybersecurity requirements of the CRA. If they do so, they can also be deemed to meet the specific cybersecurity requirements of the AI Regulation. [Recital 29, Art. 8]
- Delegated Regulation (EU) 2022/30, which complements Directive 2014/53/EU on the making available on the market of radio equipment, sets out essential requirements for radio equipment – e.g. mobile phones, laptops, alarm systems – (1) to protect the network from harm, (2) to protect personal data and user privacy, and (3) to protect against fraud. These requirements are to apply until the horizontal cyber security requirements of the CRA apply. From then on, the requirements of the Delegated Regulation will no longer apply. [Recital 15]
- Pwde that are machinery products within the meaning of the Machinery Products Regulation and for which an EU Declaration of Conformity has been issued under the CRA are also considered to be compliant with the requirements of the Machinery Products Regulation relating to the safety and reliability of control systems [Recital 30, Art. 9].
- Pwde that are electronic health record (EHR) systems and fall within the scope of the proposed European Health Data Space Regulation [EHDS, COM(2022) 197, see **cepPolicyBrief**] must also comply with the cybersecurity requirements of the CRA. They should demonstrate the compliance of EHR systems under the EHDS Regulation. [Recital 31, Art. 24 (4).
- The Defective Products Liability Directive (85/374/EEC), currently under revision [COM(2022) 495], which establishes the principle that a product manufacturer is liable, regardless of fault for damage caused by the unsafe nature of his product, is complementary to the CRA [Recital 16].
- Issuers of "European digital identity wallets (EUid wallets)", if their wallets are also pwde, must comply with both the cybersecurity requirements of the CRA and the specific security requirements of the eIDAS Regulation [(EU) No 910/2014], which is currently under revision with a view to establishing a framework for a European digital identity [COM(2020) 281, see **cepPolicyBriefs**] [Recital 18].

10 Start of application

- The CRA shall apply 24 months after its entry into force [Art. 57].
- The obligation to report security incidents and actively exploited vulnerabilities already applies after 12 months [Art. 57 in conjunction with Art. 11].

B. Legal and political context

1 Status of legislative procedure

15.09.22	Adoption by Commission
Open	Adoption by European Parliament and Council, publication in Official Journal, entry into force.

2 Options for Exerting Political influence

Directorates-General:	DG Communication Networks, Content and Technologies
European Parliament Committees:	Industry, Research and Energy (ITRE), Rapporteur: Nicola Danti (Renew, IT)
Federal Ministries:	Interior (lead)
Committees of the German Bundestag:	Interior (lead)
Decision-making mode in the Council:	Qualified majority (adoption by 55% of Member States representing 65% of the EU population).

3 Formalities

Basis for legislative competence:	Art. 114 TFEU (internal market)
Type of legislative competence:	Shared competence (Art. 4 (2) TFEU)
Procedure:	Art. 294 TFEU (ordinary legislative procedure)

C. Assessment

1 Economic impact assessment

1.1 General assessment

Cybercrime is on the rise worldwide. While the damage caused by cyberattacks in 2015 was still around 2.7 trillion € it has more than doubled by the end of 2020.[1] The German economy alone is struggling with annual losses of around 203 billion € due to theft of IT equipment and data, espionage and sabotage and around 84% of German companies were affected by a cyberattack in 2021.[2] A large part of these costs incurred can be attributed to insecure hardware and software products. Vulnerabilities in these products regularly serve as a starting point for attacks. And the number of vulnerabilities is increasing every year: while there were 18.325 in 2020, there were already more than 20.000 in 2021.[3] The German Federal Office for Information Security (BSI) also recently reported a 10% increase in the number of security vulnerabilities in software products for 2021, with the share

[1] Nai Fovino I., Barry G., Chaudron S., Coisel I., Dewar M., Junklewitz H., Kambourakis G., Kounelis I., Mortara B., Nordvik J.p., Sanchez I. (Eds.), Baldini G., Barrero J., Coisel I., Draper G., Duch-Brown N., Eulaerts O., Geneiatakis D., Joanny G., Kerckhof S., Lewis A., Martin T., Nativi S., Neisse R., Papameletiou D., Ramos J., Reina V., Ruzzante G., Sportiello L., Steri G., Tirendi S., Cybersecurity, our digital anchor, EUR 30276 EN, Publications Office of the European Union, Luxembourg, 2020, ISBN 978-92-76-19957-1.

[2] Bitkom (2022), Press release, 203 billion euros in damage per year due to attacks on German companies, 31 August 2022.

[3] EU Commission (2022), SWD(2022) 282, Impact assessment report, Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, PART 1/3, 15 September 2022, pp. 6-8.

of critical vulnerabilities - which included the vulnerabilities in Microsoft Exchange and Log4j (a Java library) - accounting for about 13%.[4] This development shows that the markets for software and hardware apparently do not succeed, or only to a limited extent, in producing products that can be considered "cyber-safe". This is due to various deficits in these markets:

Manufacturers often see no need to develop and provide cyber-secure software or hardware products. This is due to the fact that they regularly do not have to assume (full) liability for the damage that can be caused by insecure products.[5] If a cyber security incident occurs, they only bear a fraction of the resulting costs. These include any reputational damage or costs for the provision of security patches. The large remainder must often be borne by the users of the products or by other (uninvolved) third parties. However, this means that the unity of action and liability as a constituent principle of the competitive order does not exist. This is because those economic agents who are to be regarded as the causer or responsible for a damage – here: the economic operators – do not have to pay for it in full. They therefore do not bear the full consequences of their actions.[6] The incentive to produce secure software or hardware products is also diminished by the fact that the reputational damage associated with cyber incidents is often not permanent and the user of a software or hardware product is regularly confronted with high costs[7] for switching to a competitor's product. The fact that the manufacturers can pass on costs and the injured parties are not compensated by them ensures that, from an economic point of view, too little capital flows into the development of cyber-secure pwde. To remedy this market failure, measures are needed that lead to an increased internalisation of the negative externalities.

The markets for pwde regularly show characteristics of "market for lemons". This is due to the fact that potential buyers or users are often unable, or insufficiently able, to assess or observe the cybersecurity-related properties of a pwde before purchasing or using it. They lack the necessary information for this. If they do not have this information, they are not willing to pay more for a "supposedly" cyber-secure product than for another product. The result is that those manufacturers who really want to sell secure products are forced out of the market. In the end, insecure products dominate in the long run, even when there is actually a willingness to pay for resilient products. The asymmetric distribution of information between producers and buyers/users thus leads to an "adverse selection" that does not produce sufficiently safe pwde.[8,9]

The markets for pwde are often characterised by network effects, economies of scale and a high propensity to innovate and short innovation cycles. These factors mean that manufacturers usually have a strong interest in bringing their pwde to market quickly. Elaborate and cost-intensive investments in improving the cybersecurity of their products - a product characteristic that is often not a top priority in the purchase decision - delay market entry and can therefore have a detrimental effect on competition. These factors, too, thus ensure that fewer secure pwde tend to establish themselves on the market.[10]

Misaligned incentives may also prevail on the part of buyers or users of pwde, inviting free-rider behaviour. In general, the purchase of a cybersecure pwde is associated with positive externalities. Not only the buyer benefits from the secure product, but also third parties as the overall cybersecurity level increases. However, the benefiting third parties make no contribution of their own for this additional gain in security. It also reduces their need to invest in cybersecurity themselves. Thus, both effects ultimately lead to the fact that the incentive to invest in cyber-secure products at all may turn out to be low.[11]

All of this has the effect that manufacturers tend to bring pwde onto the market that are not sufficiently cyber-secure and that customers or users at the same time do not (or cannot) demand sufficiently secure products. It is therefore absolutely necessary to remedy this situation. The Cyber Resilience Act makes an important contribution to this:

---

4 Federal Office for Information Security (2022), Die Lage der IT-Sicherheit in Deutschland 2022, October 2022.

5 Moore, T. (2010), The economics of cybersecurity: Principles and policy options. International Journal of Critical Infrastructure Protection, 3(3-4), pp. 5 and 6.

6 Eucken, W. (1952/2004), Grundsätze der Wirtschaftspolitik, Mohr Siebeck, Tübingen.

7 These can also be very high in some cases, for example if no equivalent substitute product is available.

8 Kox, H., & Straathof, B. (2014), Economic aspects of Internet security. *CPB Background Document*, pp. 13 and 14.

9 Mohaddes Deylami, H., Ardekani, I., Muniyandi, R. C., & Sarrafzadeh, H. (2015). Effects of software security on software development life cycle and related security issues, p. 5.

10 Asghari, H., van Eeten, M., & Bauer, J. M. (2016). Economics of cybersecurity. Handbook on the Economics of the Internet.

11 Kox, H., & Straathof, B. (2014), p. 26.

1.2 Establish uniform cybersecurity requirements

Requiring manufacturers, importers and distributors of pwde to meet basic cybersecurity requirements and ensuring that cybersecurity is considered at the design, development and manufacturing stages of a product addresses three of the four market failures described above.

Firstly, disincentives on the part of economic actors can be effectively prevented. They have to invest more in the cybersecurity of their products, which potentially reduces the damages or costs that their customers or (uninvolved) third parties have to bear due to insecure pwde. Action and liability are again increasingly aligned and the possibilities for passing on costs are reduced. The additional obligations thus ensure a certain internalisation of negative (network) externalities.

Secondly, harmonised cybersecurity requirements create a level playing field and there are no longer potential disadvantages in the market for those economic actors who, for example, proactively provide secure products and, as a result, enter the market with their product late. Cybersecurity as an essential basic element of a pwde can no longer be penalised by the market, for example due to higher production costs or late market entry but is established as a central competitive factor.

Thirdly, uniform cybersecurity requirements prevent free-rider behaviour on the part of pwde buyers. They can now be sure that other buyers also purchase or have purchased cybersecure products and thus benefit from positive externalities. At the same time, however, they can no longer escape responsibility for a cyber-secure environment, as fewer "insecure" products will be available.

1.3 Recourse to the New Legislative Framework

Many products placed on the market in the EU must meet certain safety, health or environmental requirements. This is done using the New Legislative Framework (NFL), which sets out basic rules for product regulation in the EU.[12] It works on the principle that products must achieve certain safety objectives before they can be placed on the market, but without technically specifying en détail how these objectives are to be achieved.[13] It is based in particular on the assessment of the conformity of products with the respective requirements by the manufacturers themselves or by third parties, market surveillance by supervisory authorities, technical documentation of the product's properties and CE marking. The fact that the Commission also uses this framework, which has been in force since 2010, for the CRA facilitates the implementation of the extensive cyber security requirements enormously. This is because the manufacturers of Pwde are already familiar with it in many cases, apart from some software developers[14] , and can therefore build on established procedures and processes.

1.4 Scope of application

The fact that the Commission has chosen a very broad scope of application for the cybersecurity requirements, including not only hardware products but also non-embedded and embedded software as well as components, is appropriate, even though this will pose major challenges for a large number of economic actors and especially small and medium-sized enterprises (SMEs).[15] This is because security vulnerabilities in pwde are not a phenomenon that is limited to certain products or product types/categories. Moreover, even pwde that are actually considered non-critical and are used in supposedly secure environments can serve as a gateway and contribute to the rapid spread of a vulnerability. Furthermore, before a pwde is placed on the market, it is often not clear by whom, for what purposes and in which environment it will be used. Uniform minimum requirements for all pwde, regardless of their criticality, can therefore contribute to a noticeable increase in the level of cyber security. Nevertheless, two aspects should be considered more carefully. Firstly, a large proportion (over 90%) of manufacturers of pwde are SMEs, which, especially if they develop software products, are not yet familiar with the prescribed product testing processes, including conformity assessment. It is unrealistic to expect these SMEs to be able to adjust to these procedures satisfactorily within two years and to build up specific know-how. A

---

12 Legal acts based on the NLF have so far been adopted for numerous products marketed in the EU. This now concerns more than 20 sectors. These include electrotechnical products, toys and medical devices [SWD(2022) 282, PART 2/3, Annex 11].

13 EU Commission (2016), Guide to the implementation of EU product legislation 2016 ("Blue Guide"), C/2016/1958.

14 This is due to the fact that software is often not considered a product so far and therefore there are hardly any product requirements for it under the NFL.

15 According to the Commission, the number of companies in the software market in the EU in 2019 was approximately 366,000, over 99% of which were SMEs. The number of hardware product manufacturers in the same year was around 22,800. These are also predominantly SMEs, with over 97% [SWD(2022) 282, PART 2/3, pp. 24 and 25].

longer implementation period should be considered here, at least for those product categories that are considered less critical. Secondly, the handling of commercial open-source software should be reconsidered. It is true that their security is also central to cyber-resilient European economies. However, since their development is usually only on the shoulders of a few people, is often voluntary and requires little capital, expensive product testing procedures would often lead to their development no longer being profitable. At the same time many software products are based on open source products, there would be a danger that software development in the EU could at least stutter. Therefore, in the further legislative process, a balance must be struck between the justified desire for a higher level of cyber security and the maintenance of incentives for the development of free, open-source software.

The fact that the Commission is grading the depth of regulation depending on the criticality of the product and prescribing stricter conformity assessment procedures for "more critical" products is appropriate in principle and further strengthens resilience to cyber incidents. However, both the procedure for classifying the pwde and the classification itself are questionable:

Firstly, the Commission's classification of products into class 1 and class 2 for critical products, which it has already done, is opaque. In particular, it is not clear which criteria it has used for the classification into the two groups and what exactly the distinction between a class 1 and a class 2 product is, although the classification has real consequences, in particular with regard to the stringency of the conformity assessment. If certain pwde were already defined as critical products in the primary legislation and divided into different risk classes, this would in any case require a more thorough substantiation.

Secondly, the right given to the Commission to define further critical products is accompanied by veritable legal uncertainties. Admittedly, it is given various criteria, such as testing the cyber functionality of the pwde or the extent of losses or disruptions already caused by the use of a pwde. This is useful to prevent arbitrary decisions. However, it is not clear from the specifications which factors are decisive for classification as Class 1 vs. Class 2 and whether the criteria are given a different weighting. This should be clarified.

Thirdly, the classification is not conclusive. In many cases, the pwde in the two classes are not to be regarded as critical per se and under all circumstances. Instead, their criticality depends in particular on who uses them, under which conditions and in which (sensitive) environments. For example, the use of pwde by critical infrastructure operators in the provision of their specific services can at least serve as an indicator that increased caution is required. In addition, if a disruption or failure of the pwde could have a massive impact on the functioning of the society, this should be a signal to impose stricter requirements on their cybersecurity. However, if a pwde is used in a less critical environment, it is not necessary to classify it as "critical" straight away. The classification of pwde into criticality levels should therefore still be based much more on these factors. This would reduce the effort for the manufacturers of the pwde associated with the cyber security requirements, without at the same time making significant sacrifices in increasing cyber resilience.

1.5 Product life cycle perspective

The NFL usually focuses on the specification of product requirements that must be fulfilled before a product is placed on the market. Whether the product also fulfils subsequent requirements, for example with regard to its security, is of secondary importance. With regard to the cyber security of pwde, the CRA now takes a perspective that considers the entire product life cycle of the products. Accordingly, the manufacturer of a pwde still bears responsibility for his product even if it is already in use. This is also the right way to go. Firstly, cyber risks regularly appear during the use phase of a pwde, which cannot be anticipated ex ante or can only be anticipated with difficulty. Even with the greatest efforts, a manufacturer cannot rule out the possibility that his product has a vulnerability. Secondly, software products in particular are often equipped with new features during their life cycle, which can harbour new risks that must be addressed accordingly ex post (i.e. after they have been placed on the market). The life-cycle approach thus reduces misaligned incentives on the part of product manufacturers and counteracts associated market deficits.

1.6 Vulnerability management

The welcome life-cycle approach also includes the obligation to address and remedy vulnerabilities - including through security updates - over the expected product lifetime of the pwde or over five years from the time the product is placed on the market, whichever is shorter. This defines precisely for manufacturers how long they are obliged to deal with the cyber security of their products. This firstly creates legal certainty on the part of the manufacturers, secondly increases the confidence of users in the product quality and thirdly ensures that the

interest of manufacturers in cyber security does not dwindle too quickly even after the product has been placed on the market. Five years as the maximum period for the obligation to address vulnerabilities is a well-balanced compromise. It ensures that while resources are tied up for a certain period of time with manufacturers to strengthen the security of "old" products, this commitment does not at the same time lead to a lack of product innovations or undermine the incentive to switch to newer pwde that promise a higher level of security. The 5-year period also prevents manufacturers from having to invest unnecessary resources in the long term to keep pwde up to date, even though they have not established themselves on the market at all.

In the further negotiation process, however, clarifications should still be made as to how the term "expected life" is to be understood. While this appears to be clear and easy to define or determine in the case of a physical pwde, this is not always the case, especially in the case of software products. For these products, the question regularly arises whether a new software version is only an update of the "old" software or an upgrade, so that ultimately a "new" software product is put on the market and the product life of the old software thus ends. Clarifications in this regard would in any case contribute to increasing legal certainty for manufacturers. They could, for example, be based on whether the software product is changed to a "significant extent". Furthermore, coherence with other EU legal acts should be ensured in order to prevent contradictory regulations. For example, the rules recently presented by the Commission in its proposal for a Directive on liability for defective products [COM(2022) 495] could be interpreted as requiring updates to be made available for up to ten years, significantly longer than the CRA proposal. Furthermore, recently presented new eco-design requirements[16], which are to apply to smartphones, tablets and mobile phones, stipulate, for example, that manufacturers or importers of these products must continue to provide security, correction and function updates for the operating system used free of charge for up to 5 years after such a product has been withdrawn from the market, which does not ensure consistency with the requirements of the CRA.

1.7 Delivery without known vulnerabilities

The CRA proposal obliges manufacturers to only deliver pwde that are not known to have an "exploitable vulnerability" at the time they are placed on the market. If such a vulnerability is known, the product must not be delivered. The requirement is coherent in itself, as it ensures that manufacturers must seriously endeavour to bring only cyber-secure products onto the market and thus also counteracts the false incentive, for example for reasons of innovation, to market a product as quickly as possible, even though its cyber-security is not given. Nevertheless, the provision should be tightened up. After all, it is doubtful that a manufacturer can fully guarantee that his product does not contain any of these vulnerabilities at the time it is placed on the market, especially since there is likely to be a certain time gap between the finalisation of the manufacturing process and the delivery - particularly in the case of hardware products. Furthermore, not every known and exploitable vulnerability should have to lead to a postponement of the delivery process, but only those that pose or threaten to pose a certain security risk. Otherwise, there is a risk of unnecessary and easily avoidable delays in market entry. A goal-oriented regulation would therefore be one that ensures that manufacturers must make "reasonable" efforts to ensure that their product is placed on the market as free of vulnerabilities as possible. However, they should proceed in a risk-oriented manner and be allowed to concentrate on the serious security vulnerabilities.

1.8 Transparency requirements

Setting transparency requirements, such as under what circumstances cybersecurity risks could arise when using the product or how long the user can expect security updates, enables consumers and businesses to better assess and compare the security features of pwde, and enables them to make an informed decision on whether to purchase a pwde. They are thus an essential building block in averting market failures caused by information asymmetries, a key element in ensuring effective competition between pwde manufacturers and ultimately in the emergence of a market for cybersecure pwde.

1.9 Reporting requirements

Like the Directive on measures for a high common level of cyber security in the Union (NIS 2 Directive, see **cepAdhoc**) and the Regulation on Digital Operational Resilience (DORA, see **cepPolicyBrief**), the CRA also establishes reporting obligations for the occurrence of security incidents or, in case of the CRA, for emerging

[16] BMUV and BMWK (2022): Smartphones and tablets will be easier to repair in the future, Press Release No. 161/22, Consumption and Products, 18.11.2022.

vulnerabilities in pwde. Manufacturers of pwde often have no self-interest in voluntarily reporting incidents or vulnerabilities, as this could damage their reputation and lead to a loss of trust. At the same time, such reports often have a high economic benefit, as (uninvolved) third parties can adjust more quickly to a new hazard situation and take measures to reduce risks at an earlier stage. Reporting obligations are therefore appropriate, especially as they create incentives for manufacturers to invest in the safety of their pwde a priori. However, the envisaged notification obligations of the CRA are in need of improvement for three reasons. First, the obligation to notify every exploitable vulnerability or security incident[17] is excessive. This unnecessarily ties up resources without generating much added value and means that pwde manufacturers are ultimately subject to stricter notification obligations than critical infrastructure operators. Analogous to the NIS 2 Directive, the significance of the incident or vulnerability should be taken into account here. Secondly, a one-time notification after less than 24 hours seems insufficient. Such a short-term notification can only ever contain initial rudimentary information, with which, however, both the supervisory authorities, including ENISA, the customers and other third parties are often not yet able to do much with. In the end, such an initial notification can only be a warning. This should therefore be followed at a later stage by further notifications with more detailed information, sensibly comparable as provided for in the NIS 2 Directive. And thirdly, it should be ensured that the manufacturers of pwde are not forced to send multiple notifications to several different addressees. This could happen, for example, if a pwde manufacturer is also an essential or important facility in the sense of the NIS 2 Directive, such as an energy supplying company. In this case, it might be forced to report a cyber security incident to several bodies, namely ENISA and the national supervisory authority or a national CSIRT.[18] In order to reduce the reporting burden for the companies concerned, a single notification body should suffice in such cases, which would then in turn forward the notifications to those other bodies that are in need of the information. Furthermore, the obligation to inform users about any security incidents is too broad. The focus here should also be on their significance and their direct impact on the users of the pwde.

1.10 Conformity assessment

Conformity assessments are a proven procedure of the NLF through which manufacturers can prove that their products actually meet certain product requirements. They are a key element in strengthening confidence in the security of products and a further instrument for reducing disincentives on the part of product manufacturers. The use of the already long-established assessment procedures for testing the cyber security of pwde is expedient.[19] The fact that the Commission is also pursuing a risk-based approach, which allows self-assessment by the manufacturer for the majority of pwde (approx. 90% according to the Commission) and only provides for a more stringent assessment with the involvement of independent third parties for critical products (approx. 10% according to the Commission), enables an efficient distribution of limited resources and prevents manufacturers, conformity assessment bodies and supervisory authorities from being overburdened.

The Commission wants to enable manufacturers to make use of harmonised EU standards in particular in the context of conformity assessment, which concretise the basic cybersecurity requirements of the CRA proposal that are not aimed at a specific product or technology. This is purposeful, because the application of the product-specific detailed technical requirements anchored in these standards makes it much easier for manufacturers to prove the conformity of their products. This significantly reduces the compliance burden, increases legal certainty for manufacturers and ensures uniform application of the legislation. The use of technical specifications or other solutions, for example, is regularly associated with greater effort on the part of product manufacturers and is associated with greater uncertainties. However, it is questionable whether the use of harmonised EU standards will succeed at the time of the first application of the regulation. For it is hardly realistic that the Commission, together with the relevant standardisation organisations and bodies, will be able to draw up the necessary standards within two years for such a large number of pwde and finalise them in time. It would therefore be worth considering linking the initial fulfilment of the cybersecurity requirements of the Regulation more closely to the actual existence of the EU standards. However, such a coupling should not tempt to unnecessarily delay the standardisation process and ultimately the fulfilment of the CRA's requirements.

---

17 It is also noticeable that the Commission proposal lacks a definition of the term "security incident". However, such a definition can be found in Article 4 of the NIS 2 Directive.

18 Furthermore, if a security incident results in a personal data breach, Article 33 of the General Data Protection Regulation (GDPR) requires the controller to notify the competent data protection supervisory authority within 72 hours at the latest; i.e. there is potentially another addressee to whom notifications must be sent and again another deadline for notifications.

19 However, as noted above, the classification of Pwde into the different risk groups should be reconsidered.

1.11 Market surveillance

Uniform, cross-sectoral cybersecurity requirements for Pwde are only effective as long as it is ensured that they are actually implemented and lived by the economic actors concerned. For this, market surveillance is essential to ensure that pwde that are not considered cybersecure are not allowed to circulate in the EU internal market. The Commission's reliance on the existing, well-balanced system within the framework of the NLF is appropriate, because the market surveillance regime ensures in particular that pwde which are deemed not to be cyber-safe by a national market surveillance authority may no longer be placed on the market in the entire EU internal market or must be withdrawn from circulation. This ensures a uniform level of protection within the EU, counteracts distortions of competition and inconsistent trading conditions, and creates incentives for manufacturers to proactively consider the cybersecurity of products in the context of product design and development. The latter is also ensured by the thoroughly deterrent sanction regulations. However, should a national market surveillance authority not (be able to) perform its tasks adequately, for example due to a lack of resources or possible conflicts of interest, the diversions via Commission intervention - in cooperation with ENISA - to intervene in exceptional cases and define product-specific remedies offers additional protection that can strengthen cyber resilience in the EU.

1.12 Start of application

The Commission proposal foresees that the CRA should apply already two years after its entry into force. This timetable is understandable due to the high threat level and the economic damage caused by cyberattacks. The sooner pwde are cyber-secure, the better. Nevertheless, despite the urgency of the problem, the timetable seems too ambitious and should be reconsidered. Firstly, it is not to be expected that sufficient expertise, know-how and personnel can be built up on the part of the manufacturers as well as on the part of the notified bodies and supervisory authorities in this short time to be able to guarantee adequate compliance, testing and monitoring of the cybersecurity requirements. Considering that the number of hardware and software products covered is extremely large and, even if no more than 10% of pwde are considered critical products and thus should be subject to more stringent compliance assessments, these are still not exactly few. Secondly, more than 90% of manufacturers are SMEs or even micro-enterprises, which, if they are software developers, have little or no familiarity with obligations regarding product requirements. Thirdly, it is not certain that (European) standards and technical specifications for certain products or product categories will be available in a timely manner to an extent that allows for proper conformity assessments. For the reasons mentioned, a later start of application would be advisable. If necessary, a staggered implementation should be considered, whereby the CRA requirements for pwde used in critical areas, such as by critical infrastructure operators, apply earlier than for other pwde. This would also counteract a possible overload of the actors involved shortly before the start of the application phase of the CRA.

2 Legal assessment

2.1 Competence

The legal basis of the CRA is the approximation of laws in the internal market [Art. 114 TFEU]. According to this article, the EU may take the measures to further develop the internal market. The CRA aims to enable the free movement of products with digital elements by establishing harmonised cybersecurity requirements for these products in all Member States. The subject matter and the objective of the regulation meet the requirements of Art. 114 TFEU. Therefore, the competence is given.

2.2 Subsidiarity and proportionality vis-à-vis the member states

Trade in pwde often has a cross-border character. Even pwde imported into the EU are mostly distributed in more than one member state. Moreover, pwde often use remote data processing and network solutions, so that it is not possible to limit or restrict the use of the product geographically. Technical possibilities allow data to be transferred to other devices in seconds, as well as connections between electronic components and systems without physical contact with the device. As a result, a low level of cyber security even in a single element

threatens with widespread impact. Actively exploited cybersecurity vulnerabilities and incidents can have an impact on several member states or even the entire single market, that is why EU-wide regulation is reasonable.[20]

Due to the lightning fast spread of data within pwde to distant parts of the world, different national laws as well as existing legal loopholes create legal uncertainties and obstacles. Since a spatial delimitation of the use of pwde would hardly be possible and counterproductive, this argues against the introduction of comparable measures by the individual EU member states. For an effective and open internal market, uniform legal standards are necessary for all pwde placed on the market in the EU. Other measures, such as non-legislative projects, cannot nearly achieve the level of cyber resilience as a binding legal act such as the CRA, and would therefore be less effective. Hence, the adoption of a regulation at the supranational level is an optimal solution. Against this background, subsidiarity and proportionality vis-à-vis the member states are not problematic.

Nonetheless, the proportionality of some provisions may be questioned. At first sight, the envisaged start of application of the CRA may seem late, as the need to strengthen cybersecurity already exists today. Many security incidents may occur as well as vulnerabilities may be discovered in the two years until the start of application of the CRA. Without the applicable law, it is likely that such incidents would not be prevented due to a lack of action of the pwde manufacturers and the other economic actors involved. However, adapting and implementing necessary measures to meet the numerous requirements of the CRA can be challenging, especially for manufacturers who have years-long development cycles for their pwde.

2.3 Other compatibility with EU law

Under the CRA proposal, the Commission may amend or supplement certain parts of the CRA by means of delegated acts. According to Art. 290 TFEU, the Commission may adopt non-legislative acts to amend non-essential elements of a legislative act or to supplement it with non-essential elements. However, the article does not clearly regulate which parts of a legislative act can be considered essential and which non-essential. European case law does not provide a clear answer to this either. In the case law of the ECJ, Article 290 TFEU is interpreted in a way that the adoption of a regulation dealing with the essential aspects of a matter requires "political choices" which "fall within the Union legislator's own competence."[21] Such essential aspects are thus reserved for decision by the European Parliament and the Council.

Within the framework of an inter-institutional agreement, the European Parliament, the Council and the Commission have drawn up non-binding criteria for the application of Art. 290 TFEU.[22] These indicate that additional rules building on or developing the content of the basic act can be established by means of delegated acts. However, there are no explanations on how political and thus essential decisions differ from technical and thus non-essential decisions. Ultimately, it must therefore be examined on a case-by-case basis whether an apparently technical aspect could have political significance upon closer examination.

Against this background, some provisions of the CRA can be seen as problematic. It refers to the provisions that grant the Commission the right to determine by means of delegated acts which pwde are to be classified as critical (classes I and II) and as highly critical [Art. 6 para. 2 sentence 1, para. 3 and 5]. This power gives the Commission the right to specify the scope of the CRA more precisely. In essence, it also decides which pwde are subject to a stricter legal framework and which enjoy more favourable treatment. In particular, the stringency of the required conformity assessments increases with the classified criticality of a pwde.

Whether the additions or adjustments to the classification of categories of pwde as critical, highly critical or non-critical, which at first glance appear to be technical, as well as whether they can and will be made completely free of political considerations, cannot be clearly predicted. At least it may be doubted. The CRA indeed prescribes criteria that the Commission must use as a basis for classifying the criticality of a category of pwde, so that arbitrary and unfounded classification decisions can be ruled out. However, the Commission retains a certain degree of discretion in the classifications, as the CRA proposal does not contain any clear and unambiguous specifications on how the distinction between Class I and Class II pwdes, and between critical and highly critical pwdes, is to be made. For example, although the Commission lists 5 criteria for classification into Classes I and II,

---

[20] Judgment of the Court (Grand Chamber) of 2 May 2006, United Kingdom of Great Britain and Northern Ireland v. European Parliament and Council of the European Union, Case C-217/04, para. 63.

[21] Judgment of the Court (Grand Chamber) of 5 September 2012, Parliament v Council, C-355/10, EU:C:2012:516, para 65.

[22] Non-binding criteria of 18 June 2019 for the application of Articles 290 and 291 of the Treaty on the Functioning of the European Union (hereinafter Non-binding criteria for the application of Articles 290 and 291), 2019/C 223/01, OJ C 223/1.

it does not specify which criteria must be met to what degree for a product to fall into either Class I or II. In addition, the Commission does not have to provide an argumentation for the classification of pwde into the risk groups. It is therefore also not transparent which criteria it will use, to what extent, or which criteria will have priority to.

Ultimately, it is therefore quite conceivable that the classification of a category of pwde into a certain risk group is not a purely technical decision in practice, even if the Commission strictly adheres to the catalogue of criteria specified in the CRA. This is true if only because the use of a certain pwde in a sensitive environment, i.e. for example by an operator of a critical infrastructure, can be highly political, as the experience has shown. The ongoing discussion about the use of technology from the telecommunications supplier Huawei, for example, in the expansion of the 5G network, is worth mentioning here. In such cases, it could be politically expedient or opportune to carry out a higher risk classification and to apply stricter testing standards to cyber security, although this might not be (absolutely) necessary in every case from a purely technical perspective. Should the Commission therefore be given the power to independently classify pwde into risk groups, it can be assumed that such decisions may be not of a purely technical nature, but that political considerations will also play a role, including those that create additional barriers to market entry, e.g., if the pwde concerned are largely manufactured abroad.

Despite the above-mentioned problems that could accompany the delegation of powers, such possibility of amending the legislative act also has advantages. In legal terms, delegated acts are an effective instrument that help to keep legislation up to date. By means of a legal norm delegating to the Commission the right to adopt its own legislative acts, the legislator can determine the procedure for legislative adjustments in designated areas. The adoption of a delegated act is clearly a faster and simpler option than the diversions via an ordinary legislative procedure. Considering delegated acts, the Commission can react quickly to market changes and the emergence of new technologies and pwde. Within this legal tool, it can quickly identify new critical or highly critical pwde and update the lists for categories of critical or highly critical products.

D. Conclusion

With the CRA, the EU Commission has presented an ambitious legal framework to increase the cybersecurity of products with digital elements. Hence, the Commission should be congratulated on this successful legal act. The CRA makes a significant contribution to remedying numerous deficits inherent in the markets for these products. The CRA will encourage manufacturers of pwde to invest more in the cybersecurity of their products and counteract existing disincentives in this respect. It will also enable potential buyers of pwde to closely consider the cybersecurity of the products in their purchasing decisions. However, some of the proposed regulations still need fine-tuning. For example, the Commission's classification of products into classes 1 and 2 for critical products is opaque and inconclusive. The delegation of power to the Commission to adopt delegated acts on the adaptation of the lists for (highly) critical products is also not unproblematic from a legal point of view, because political considerations could easily come into play here in the Commission's decisions. Furthermore, coherence with other EU legal acts is not yet given in some cases, such as the duration of the obligation to rectify vulnerabilities, which deviate from recently established eco-design requirements for smartphones, tablets and mobile phones. Finally, it must also be examined whether the start of the CRA's validity of two years after its entry into force is not too ambitious. Regardless of the urgency to strengthen cybersecurity in the EU, the challenges for economic actors and supervisory authorities should be concerned.

E. Annexes

1 Annex I: Products with digital elements

Non-critical pwde (i.e. all pwde that are not critical or highly critical pwde), e.g.	Critical pwde (Class 1)	Critical pwde (Class 2)	Highly critical pwde
Smart speakers	Identity Management System Software and User Access Control Software	Operating systems for servers, desktops and mobile devices	Still open
Word processing	Standalone and embedded browsers	Hypervisors and container runtime systems with visualised operating systems	
Photo editing	Password manager	Public key infrastructure and issuer of digital certificates	
Computer games	Software that searches for, removes or secretes malicious software	Firewalls and prevention systems for industrial use	
Hard disks	Products with digital elements with the function of a virtual private network (VPN)	Microprocessors for general purposes	
	Network management systems	Microprocessors for integration in programmable logic controllers and safe elements	
	Tools for managing the network configuration	Routers, modems for connection to the Internet and switches for industrial use	
	Systems for monitoring network traffic	Fuse elements	
	Network resource management	Hardware Security Modules (HSM)	
	SIEM systems (Security Information and Event Management)	Secure cryptoprocessors	
	Patch or update management	Smartcards, smartcard readers and tokens	
	Management systems for application configuration	Industrial automation and control systems (IACS) used by critical facilities	
	Remote access / release software	Industrial Internet of Things devices used by critical facilities	
	Mobile device management software	Products for giving sensor capabilities to robots, actuators and robot controllers	
	Physical network interfaces	Smart meters	

	Operating systems not falling under Class II		
	Firewalls, attack detection and/or attack prevention systems not included in Class II		
	Routers, modems for internet connection and switches not falling under class II		
	Microprocessors not falling within Class II		
	Microcontroller		
	Application specific integrated circuits (ASIC) and field programmable gate arrays (FPGA) used by critical facilities		
	Industrial automation and control systems (IACS) not included in Class II		
	Industrial Internet of Things not falling under Class II		

2 Annex II: Conformity assessment procedures to be applied

Conformity assessment procedure based on internal control (Module A)

The manufacturer must

- ensure and declare on its own responsibility that the pwde complies with all basic cyber security requirements,
- prepare a technical documentation,
- Take all necessary measures to ensure that the design, development, manufacturing and vulnerability management processes and their monitoring are compliant with the essential cyber security requirements,
- affix the CE conformity marking on each compliant pwde,
- issue a declaration of conformity for each pwde and keep it for ten years after the product has been placed on the market.

EU type-examination (module B)

During EU type-examination, a notified body examines and attests the technical design and development of the pwde and the procedures put in place by the manufacturer to deal with vulnerabilities.

Manufacturers may appoint a notified body of their choice. This body shall examine the technical documentation and additional evidence submitted as well as the samples of one or more important parts of the product (combination of design and construction samples), in particular whether products or samples and processes set up comply with the harmonised standards and/or technical specifications.

The notified body shall draw up an assessment report in which it shall present the results of the examinations carried out. Publication of the report shall be subject to the agreement of the manufacturer.

If the type and the procedures for dealing with vulnerabilities comply with the requirements, the notified body may issue an EU type-examination certificate to the manufacturer. The certificate shall contain all relevant information demonstrating conformity.

Manufacturers shall inform the notified body of any changes to the approved type and procedures for dealing with vulnerabilities. Such modifications shall require additional approval in the form of an addition to the original EU type-examination certificate.

Conformity to type based on internal production control (Module C)

In this conformity assessment procedure, the manufacturer shall take all measures necessary to ensure that the manufactured pwde is in conformity with the approved type described in the EU-type examination certificate and satisfies the essential cyber security requirements.

The manufacturer must also affix the CE marking to each pwde that conforms to the type described in the EU type examination certificate and meets the cybersecurity requirements. He must also draw up a declaration of conformity for each pwde product model and keep it for ten years after placing it on the market.

Conformity assessment procedure based on full quality assurance (module H)

In this conformity assessment procedure, the manufacturer declares on his own responsibility that his pwde and vulnerability management procedures are compliant with the requirements.

Manufacturers shall operate an approved quality system for the design, development and manufacture of the pwde and for the management of vulnerabilities and shall maintain its effectiveness throughout the whole life cycle of the product concerned. The quality system shall be reviewed and approved by a notified body.

Manufacturers must inform the notified body of any intended change to the quality system. The body shall examine the changes and shall decide whether a reassessment is necessary.

Manufacturers shall ensure that notified bodies are able to verify that they duly fulfil the obligations arising out of the approved quality system. The bodies shall also carry out periodic audits for this purpose.

Manufacturers must affix the CE marking to each pwde that complies with the requirements. They must also draw up a declaration of conformity for each pwde product model and keep it for ten years after placing it on the market.