CYBER RESILIENCE ACT

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.

cep**PolicyBrief** No. 1/2023

SHORT VERSION [Go to Long Version]

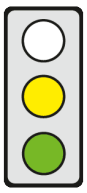
Context | Objective | Interested Parties

Context: Software and hardware products have been increasingly subject to cyberattacks in recent years. One of the main causes is the low level of cybersecurity of these products. In 2021 alone, losses amounting to € 5.5 trillion were incurred worldwide. The Commission is therefore proposing a Cyber Resilience Act (CRA).

Aim: The Commission wants to establish uniform cybersecurity rules for manufacturers, importers and distributors of products with digital elements (PWDEs). PWDE manufacturers are to improve the cybersecurity of their products as early as the design and development phase. Furthermore, transparency regarding the security features of PWDEs is to be enhanced.

Affected parties: Manufacturers, importers, distributors and users of PWDEs, conformity assessment bodies.

Brief Assessment



Pro

- The Cyber Resilience Act makes a significant contribution to strengthening cybersecurity in the EU. It addresses, in a targeted manner, several deficits in the markets for PWDEs.
- Uniform cybersecurity requirements will counteract false incentives among manufacturers, importers and distributors of PWDEs who now have to bear a greater share of the costs associated with unsafe PWDEs. It will be more difficult to pass the costs on to customers and third parties.
- The transparency requirements will make it easier for buyers of PWDEs to assess and compare their safety features.
- Setting a timeframe for fixing vulnerabilities gives PWDE users more confidence in product quality.

Contra

- The classification of critical products into two classes, already undertaken by the Commission, is non-transparent and inconsistent. There are PWDEs in both classes which cannot be considered critical per se.
- The classification of PWDEs according to their criticality cannot be regarded as a purely technical decision free from political considerations. The delegation of powers to the Commission to adopt delegated acts on classification is therefore at least questionable.
- The envisaged start date - 2 years after entry into force of the CRA - is too ambitious.

General Evaluation [Long Version C.1.1]

Commission proposal: A legal framework for the development and distribution of cybersecure products with digital elements (PWDEs) will be established in the EU.

cep-Assessment: PWDE manufacturers regularly bring out products that are not cybersecure. At the same time, it is difficult for buyers of PWDEs to demand safe products due to various deficits in the markets for PWDEs, such as false incentives on the manufacturing side and a lack of information available to buyers. The CRA will make a tangible and significant contribution to addressing these market deficits.

Authors: Anastasia Kotovskaia, LL.M. and Philipp Eckhardt | kotovskaia@cep.eu
cep | Kaiser-Joseph-Strasse 266 | 79098 Freiburg | Telephone +49 (0)761 38693-0 | www.cep.eu

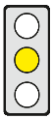
Uniform cybersecurity requirements [Long Version C.1.2]

Commission proposal: Manufacturers, importers and distributors of PWDEs will have to comply with basic cybersecurity requirements. Sufficient attention must already be given to cybersecurity in the design, development and manufacturing stages of a product.

cep-Assessment: Uniform cybersecurity requirements will counteract false incentives among manufacturers, importers and distributors of PWDEs. In future, they will have to invest more in the cybersecurity of their products. This will reduce the costs which up to now customers and third parties have often had to bear as a result of insecure PWDEs. In addition, the competitive disadvantages incurred by economic actors who are proactive in providing safe products will be reduced, and free-riding among PWDE buyers will be more difficult.

Scope [Long Version C.1.4]

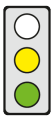
Commission proposal: The CRA applies to products with digital elements (PWDEs). These are, most notably, connectable software or hardware products. PWDEs are divided into four groups: (1) Non-critical PWDEs, including hard disks and computer games, (2) Critical PWDEs (Class I), including browsers and password managers, (3) Critical PWDEs (Class II), including operating systems for servers, routers and smartcards, and (4) as yet unspecified highly critical PWDEs.



cep-Assessment: Defining the scope as very broad is appropriate because vulnerabilities can occur in many, even supposedly non-critical PWDEs. However, the classification of critical products into 2 classes, which has already been undertaken, lacks transparency. In addition, the classification is inconsistent because there are many PWDEs in both classes which cannot always be regarded as critical per se. In fact, their criticality depends on where they are used, by whom and under what conditions.

Vulnerability management [Long Version C.1.6]

Commission proposal: PWDE manufacturers must ensure that vulnerabilities are addressed for the expected lifetime of the product or for five years from the date the product is placed on the market, whichever is shorter.



cep-Assessment: Setting a time frame for manufacturers to fix vulnerabilities gives PWDE users more confidence in product quality. However, coherence with other EU legislation, regarding the duration of the duty to fix vulnerabilities, is not yet in place, in particular vis-à-vis the proposal for a Directive on liability for defective products and the new eco-design requirements for smartphones, tablets and mobile phones.

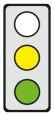
Transparency requirements [Long Version C.1.8]

Commission proposal: PWDE manufacturers must provide information to product users, such as the circumstances in which cybersecurity risks may occur when using the PWDEs, for how long security updates will be provided, and the company contact point where information about vulnerabilities can be reported.

cep-Assessment: Transparency requirements make it easier for consumers and companies to classify and compare the safety features of PWDEs. This allows them to make an informed decision about acquiring a PWDE. Such requirements therefore contribute to reducing market failures caused by information asymmetries.

Reporting requirements [Long Version C.1.9]

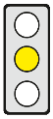
Commission proposal: PWDE manufacturers must report any cybersecurity incident or actively exploited vulnerability to the European Union Agency for Cybersecurity (ENISA) within 24 hours.



cep-Assessment: PWDE manufacturers are often reluctant to report cybersecurity incidents or vulnerabilities voluntarily due to reputational risks. However, such reports often have a major economic benefit as steps can be taken to reduce the risk at an earlier stage. Reporting obligations are therefore appropriate. Nevertheless, the obligation to notify any exploitable vulnerability or any security incident is excessive. As with the NIS 2 guideline, their significance should be taken into account.

Classification of PWDEs according to their criticality [Long Version C.2.3]

Commission proposal: The Commission may, by means of delegated acts, add new categories of critical products to the lists of critical PWDEs or remove categories from those lists. Thus, it can also create a list with categories of highly critical PWDEs. Its decision is based on several criteria, such as whether the PWDE is used by critical infrastructure operators.



cep-Assessment: The fact that the Commission can create lists of (highly) critical PWDEs by way of delegated acts means that its decisions lack transparency. Furthermore, the degree to which the criteria must be met is not specified. Such delegation of power to the Commission produces a risk that the classification of PWDEs could be influenced by political considerations.