European Commission
attn. Mr M. Šefčovič, Vice-President for Interinstitutional Relations
and Foresight
Wetstraat 200
1049 Brussels
Belgium

date *13 December 2022*
subject *Proposal for a Regulation on horizontal cybersecurity requirements (COM(2022) 454)*
our reference *172339U*

COURTESY TRANSLATION

Dear Mr Šefčovič,

In their committee meeting of 15 November 2022, the members of the standing committee for Justice and Security of the Senate of the States General discussed the European Commission's proposal for a Regulation on horizontal cybersecurity requirements (also known as the Cyber Resilience Act).[1] The members of the parliamentary parties of the GreenLeft Alliance (**GroenLinks**), the Labour Party (**Partij van de Arbeid/PvdA**), the Socialist Party (**Socialistiche Partij/SP**) and the Animal Rights Party (**Partij voor de Dieren/PvdD**) together have a number of questions about the proposal. The member of the parliamentary party of the Independent Senate Group (**Onafhankelijke Senaatsfractie/OSF**) also has questions about the proposal.

Questions jointly raised by the members of the GroenLinks, PvdA, SP and PvdD parliamentary parties

The members of the GroenLinks, PvdA, SP and PvdD parliamentary parties have taken note with interest of the proposal. They support the principle that there should be clear general frameworks for the security of digital products and services. However, the members have a number of questions, for example about the impact of the Regulation on free and open-source software and about the effective enforcement of the proposal.

Free and open-source software

The members are pleased to note that recital 10 of the proposal states that free and open-source software, developed or supplied outside the course of a commercial activity should not be covered

[1] COM(2022) 454.

by the Regulation.[2] However, they would point out that the development of free and open-source software is carried out in very diverse ways. They are therefore concerned that what constitutes free and open-source software developed or supplied in the course of a commercial activity is not sufficiently clearly defined. Does the European Commission agree that it is essential for open-source software developers to be given clarity about the applicability of the Regulation in order to ensure that it has no unforeseen consequences for open-source software in Europe? What were the considerations that led the Commission to adopt this text of the present proposal?

The members are pleased that the recitals also give a number of examples of what may constitute a commercial activity in the case of software. They would like to know whether the European Commission considers that the following examples could also be largely covered by the term 'commercial activity':

1. receipt of voluntary and unconditional donations from users of the software;
2. receipt of performance-related donations ('feature bounties');
3. sponsorship of developers, for example in the form of materials received or the reimbursement of travel expenses when attending conferences;
4. the free loan of equipment to promote the development of open-source software.

Naturally, there will also be (large-scale) free and open-source software projects that do fall within the scope of the Cyber Resilience Act (CRA). The members do not, of course, find this objectionable: after all, large-scale open-source projects that are money spinners must also be secure. However, the members consider that some aspects of how this is to be implemented are unclear. Who is responsible for compliance with the obligations in Chapter II of the proposal if a software product made by a collective is 'placed on the market' by a market participant[3], for example by a firm that provides paid support services?[4] Is it the market participant which provides the support services, is it the collective of volunteers who write the software, or is it both? Is it possible under the current proposal for a single volunteer to be held liable because the software to which he contributed is being marketed by a third party?

The members consider it important for the concerns of the free and open-source software community to be addressed and for Union citizens to be properly informed about when a product or software project will fall under the terms of this proposal. This is to prevent chilling effects and alleviate the administrative burden. What action will the European Commission take to ensure that the effects of the Regulation are clear and that it remains possible for the free and open-source software community to gauge the administrative burden of complying with its provisions? Could the Commission provide concrete assistance to the free and open-source software community by drawing up

[2] COM(2022) 454, p. 15.

[3] Article 3 (21), p. 34.

[4] Recital 10, p. 15.

guidelines on when, and to what extent, open-source software projects will fall within the scope of the Regulation?
Does the European Commission endorse the importance of a healthy and active open-source software community in Europe, both from the perspective of reducing dependence on software from outside Europe and from the perspective of digital innovation? If so, has the Commission taken, or is it planning to take, any measures to create a more level playing field for open-source software and hardware in the EU?

The members would also point out that much open-source software that is made available free of charge on a non-commercial basis is subsequently used in commercial products by third parties. Much software on which many people depend (directly or indirectly) is to a large extent developed by volunteers. Has the European Commission considered including provisions in the CRA encouraging manufacturers that use open-source software to support voluntary upstream open-source software developers in complying with the obligations of the CRA? If so, why has it not implemented them? If not, would the Commission be in favour of adding such incentives to the CRA?

Enforcement
The members wonder how they should view the relationship between the CRA and the proposal for a revised Product Liability Directive. In what way does the CRA or the new Product Liability Directive provide sufficient options for end users to enforce compliance with the obligations under the CRA?

Product lifetime[5]
Members are pleased to note that the Regulation includes an obligation to remediate vulnerabilities for a specified period of time. However, given the EU's sustainability ambitions, they are puzzled by the chosen term of a maximum of five years or the expected product lifetime, if shorter. After all, many physical products are completely dependent on secure software. If the software on such products is supported for only a short period, this can lead to unnecessary waste. Why was a general term chosen rather than a product-dependent term? And what was the specific reason for choosing a maximum period of 5 years?

Moreover, users may wish to continue using a product with digital elements after the end of this statutory support period. What options does the CRA offer users to ensure that they can continue receiving security updates after the end of this period, possibly from a source other than the original manufacturer? How would the European Commission view the idea of making it obligatory for a manufacturer to make source code, including preparatory material such as toolchains and compilation data, available after a certain period of time if it no longer wishes to provide security updates?

[5] Article 23 (2), p. 47.

Questions raised by the member of the OSF parliamentary party

The member of the OSF parliamentary party has taken note of the proposal to increase digital security across the entire sector and thus make the overall ICT infrastructure less vulnerable. He sees this Regulation as conferring the right to cybersecurity and imposing an update obligation. However, he would like to have more clarification about a number of aspects that are unclear.

Scenarios

By way of addition, what route is offered to ensure that national initiatives are feasible on a European scale as well? Examples would be (additional) directives, implementing legislation and also (subsidy) schemes.

Does the European Commission consider that having in place a broader procedure would be desirable and feasible? This could include, for example, multiple consultations or the establishment of an advisory body drawn from the sector. A broader procedure, possibly even cyclical, could help in developing or continuing to develop the criteria and the provision of sector-wide information about the standard that is being pursued. And also help, within the scope of the CRA, to ensure that the procedure is and remains aligned with other EU legislative instruments. If so, how does the Commission envisage this happening?

Cybersecurity requires highly specialised knowledge which members of parliament tend to lack. This lack of expertise is especially true of this field. What has been done to ensure that the CRA will also be capable of being implemented as a policy? And what has been done to prevent this Regulation from flopping? Much trust has been lost when it comes to governments and their ICT projects. How does the European Commission intend to restore or prove its credibility, so that it also obtains sector-wide support enabling it to elevate cybersecurity to a higher level with this Regulation?

Enforcement

How the CRA is to be enforced and what will be the scope and strength of the enforcement action remains unclear in the proposal. The arsenal of resources that could be necessary could include measures that are currently the preserve of national law. Can the European Commission shed light on the legal consequences that may arise from compliance or non-compliance with the CRA?

Start-ups and innovation

The Regulation invites providers to proceed with certification and obtain a label. This also applies to start-ups and innovation within the sectors that will fall under this Regulation. A self-assessment costing an estimated EUR 18,400 and/or a third party conformity assessment costing an estimated EUR 25,000 can be regarded as sizeable investments. Does the European Commission intend to provide a subsidy scheme for this purpose? Or does it envisage introducing rules on exceptions or narrowing the scope of the Regulation to ease the administrative burden?

While European developers will be faced with the CRA, there is a good chance that globally oriented players within the sector will locate their innovation activities outside Europe. Does the European Commission have any idea of how the CRA will affect the sector's labour market and our global position within the knowledge economy? And/or is the Commission confident that this Regulation will result in the adoption of a worldwide standard with which non-European providers too may be obliged to comply? Does the Commission envisage a situation in which providers avoid the European market for the time being, owing to constraints on supply, freedom of choice and the provision of a customised product?

Fair competition

Compliance costs are estimated to be 2% of turnover. This gives a figure of EUR 29 billion on a total turnover of EUR 1,485 billion. As the cost of a self-assessment or conformity assessment is estimated to be between EUR 18.4 thousand and EUR 25 thousand, it can be deduced that for this certificate a turnover in excess of EUR 1 million is regarded as in line with market rates. Has the European Commission asked market surveillance authorities for their views?

Financial consequences

The financial consequences for central government and/or other government bodies as well as the consequences of regulatory pressure for the business community and the general public are expected to run into the billions. This is true of both costs and cost savings. Once the consequences of introducing this Regulation become clear, does the European Commission intend to set up a compensation scheme for this? If so, what target groups (such as municipal authorities or SMEs) will be compensated and for what reasons? How will this be incorporated into the budget and/or how will it be traceable?

Ransomware attacks on data and systems

In recent years, government bodies and public institutions too have had to deal with cybersecurity incidents. Can the European Commission indicate how such situations could have been prevented (for example by the Regulation)? What criteria are used, for example in procedures employed to counter ransomware attacks designed to access data and assume control of systems?

Active exploitation of weaknesses by third parties

The war in Ukraine has awakened Europe to the fact that there is also a digital front. How does Europe propose to use the Regulation to arm itself in the 'digital war'? On what restrictions on and/or freedoms of the national security and intelligence services does the CRA shed a different light?

Protection of whistle-blowers and ethical hackers
Weaknesses in systems are always discovered. Suppliers have an economic interest in ensuring that systems appear to have no weaknesses. How does this Regulation help to protect whistle-blowers and ethical hackers?

The members of the standing committee for Justice and Security await your reply with interest.

Yours sincerely,

M.M. de Boer
Chair of the standing committee for Justice and Security