APELL Association Professionelle Européenne du Logiciel Libre
The European Open Source Software Business Association

Avenue des Arts 56, 4C, 1000 Brussels, Belgium
Web: www.apell.info
Contact: apell@apell.info
Transparency No. 765379449482-59

5 Sept. 2023

Europe's Open Source Industry's Statement on the Cyber Resilience Act

The Cyber Resilience Act (CRA) is a European regulatory initiative designed to require manufacturers, distributors and importers of products with digital components to meet higher security standards for their products or services at the design stage and throughout the product lifecycle.
The European Open Source Software Business Association (APELL) explicitly supports the goals of the Cyber Resilience Act to increase the quality and security standards of IT products. The software companies represented by APELL's members have a strong interest in offering and distributing secure software and see commercial software providers with the intention of making a profit as having a responsibility in this regard. The members of APELL therefore participate in their respective European countries in various initiatives that contribute to improving the IT security of open source software.

Importance of open source software for innovation, competition, the overall economy, as well as for digital sovereignty

According to various studies, around 78-96 percent of all software products today contain open source components. This means that open source software plays a decisive role in the IT industry and in the economy as a whole - nothing works without open source. A study commissioned by the EU Commission and published in 2021 also confirms this significant influence of open source software on the competitiveness of European companies, on economic growth, on the start-up/SME scene and on Europe's technological independence. According to the study, open source makes a significant contribution to the EU's gross domestic product (GDP): Around €1 billion invested in open source by companies in the EU in 2018 resulted in an economic added value of €65-95 billion, according to the study.

The use of open source software is also of central importance for strengthening digital sovereignty in public administration as well as in business and industry. This is because open source software ensures that the systems used can be independently verified, designed and exchanged. For this reason, important projects of the European Commission to strengthen digital sovereignty rely significantly on open source software. These include among others the Open Source Strategy by the European Commission, the Open Source Observatory, its support of the European Alliance for Industrial Data, Edge and Cloud, and Horizon Europe, a research and innovation funding programme.

The difficult demarcation of "commercial open source software" in the CRA

The CRA appears to be written primarily with proprietary software in mind. Therefore, the requirements to be met are also formulated with regard to the development and distribution models of proprietary software. However, the development and distribution models of open source software differ considerably from the development and distribution models of proprietary software due to the open and cooperative approach and the freedoms granted by the software licenses. For example, although manufacturers who develop open source software may control the products they supply to their customers under commercial contracts, they have only indirect influence over the software, which can be freely downloaded by third parties and possibly modified and redistributed for entirely different purposes. They should therefore not have to be liable for third-party software that uses all or part of their original software code.

The CRA does provide an exemption for open source software, provided it is not used for commercial activities. However, the problem lies in the concrete definition of "commercial". Here, a clear demarcation is difficult and there is too much gray area with room for interpretation and thus legal uncertainty. Open source solutions are sometimes developed and maintained in the context of a purely commercial activity (by paid employees of a one or more companies with a commercial interest), in the context of science and teaching, by public administration and sometimes also by thousands of volunteers in their free time, without their own commercial interest. Often open source solutions are also developed in the context of a cooperation between many, if not all, of these different actors, so that a clear distinction between "commercial" and "non-commercial" is often not easy to make. The intertwining of voluntary and commercial actors and organizations is inherent to the open source ecosystem.

In addition, it is also not clear in the CRA whether the provision of pure services related to open source products (project work, 2nd level help desk, etc.) already qualify as commercial activity, so that the providers of such services automatically fall under the obligations of the CRA. Again, more clarity is needed. While commercial open source software providers with the intent to make a profit should clearly fall within the scope of the CRA in APELL's view, the exemption for non-commercial open source providers still needs to be improved. Attempts to date to more clearly delimit the open source exception in the CRA have not yet been able to solve the problem of impending legal uncertainty and over-regulation.

Danger of over-regulation

The CRA currently takes insufficient account of the special development and distribution models of open source, which means that regulations under the CRA are difficult to apply to open source software in many cases or result in unintentional over-regulation. The way the CRA is currently formulated, many smaller and non-commercial open source projects would also fall under the defined requirements, which they do not have the resources to meet. In fishing, the size of the meshes in the net is matched exactly to the size of the fish to be caught. In the case of the CRA, the meshes are currently far too narrow, so that too many voluntary open source initiatives, projects from research and teaching, or individuals are included in the liability that do not actually belong to the intended target group of the CRA.

Risk of legal uncertainty

The scope for interpretation and the legal uncertainty caused by the unclearly formulated open source exception mean that smaller open source projects, which usually do not have professional legal counsel at their disposal, cannot be sure whether the open source exception applies to them or not. Out of caution and to avoid unaffordable liability claims, these companies or initiatives would then refrain from open source developments if necessary. Non-European open source providers would possibly withdraw from the European market, and European companies would cease their involvement in open source projects from which industry, science and administration are currently benefiting immensely. Thus, the CRA threatens to create a chilling effect and do great damage to the entire open source ecosystem. Since countless digital products and solutions are built on open source components, a negative domino effect can be assumed for the entire software industry.

Threat of damage to economy and digital sovereignty

This would slow down SMEs and start-ups in particular, and would, more generally, have significant negative effects on competition and the speed of innovation. Since open source software also plays a central role in science, the legal uncertainty or over-regulation caused by the CRA would also have negative consequences for research and teaching as well as the transfer of innovation from science to industry. Open source foundations, which do central (non-profit) work for many open source projects, would also be threatened by the CRA.

With respect to open source software, the CRA would thus miss its target and achieve the opposite of what it was conceived for. Instead of more secure open source software, we would have less and, above all, less secure open source software.

In order to avoid these undesirable side effects, some concrete suggestions are made below as to how currently still woolly or problematic formulations can be improved so that the collaboration of commercial and non-commercial parts of the open source ecosystem under the CRA can also be enabled in the future.

1) Development Model - Recital 10

The text of the ITRE Committee from the EU Parliament states "*Whether a free and open-source product has been made available as part of a commercial activity should be assessed on a product-by-product basis, looking at both the development model and the supply phase of the free and open-source product with digital elements.*"
However, a commercial open-source software product consists of numerous components that have been developed in a wide variety of ways (including on a volunteer basis). The development process consists of a long chain and may involve several years and countless actors and organizations. The provider of the final product may have been involved in only part of the development process, or not at all. It is therefore almost impossible for the vendor to have all the information of each step in the development process and to decide whether the open source exception applies in its case or not. The complexity of the different open source development models is thus not sufficiently taken into account in the CRA at this point.
The text by the Council of the European Union therefore states more appropriately: "*The circumstances under which the product has been developed, or how the development has been financed should not be taken into account when determining the commercial or non-commercial nature of that activity.*"
The development model must not play a role in whether a product is considered "commercial". The text proposal by the Council of the European Union is therefore to be given preference in the trilogue.

2) Development and maintenance by a single organization - Recital 10a

The text of the ITRE Committee from the EU Parliament states "*For example, a fully decentralised development model, where no single commercial entity exercises control over what is accepted into the project's code base, should be taken as an indication that the product has been developed in a non-commercial setting.*
On the other hand, where free and open source software is developed by a single organization or an asymmetric community, where a single organization is generating revenues from related use in business relationships, this should be considered to be a commercial activity."
This case - open source software that is developed and maintained only by a single organization or a community dominated by the commitment of a single organization - applies to a very large proportion of software projects, especially open source SMEs. In most cases, if the software package is very small, only a single company or organization will benefit financially through distribution.
However, the consequence of this is that large companies such as hyperscalers (“GAFAM”) would benefit from the wording and, in case of doubt, it is possible for them to circumvent this requirement via subsidiaries, etc., while SMEs would not fall under the open source exception and would therefore be disproportionately harder hit in comparison.

The definition "where free and open source software is developed by a single organization..." must therefore be deleted.

3) Software developers employed by commercial projects - Recital 10a.

The text of the ITRE Committee from the EU Parliament further states in Recital 10a: "*Similarly, where the main contributors to free and open-source projects are developers employed by commercial entities and when such developers or the employer can exercise control as to which modifications are accepted in the code base, the project should generally be considered to be of a commercial nature.*"

This would automatically bring under the CRA many open source projects in which individuals participate in the development and maintenance of the software who are employed and paid for their work in that or some other context. In other words, as soon as one of the developers has any kind of job, the open source project is considered "commercial."

This definition is problematic, since many full-time developers are also involved on a voluntary basis in other open source projects, some of which are completely different. This also applies, for example, to many of the people involved in the large open source foundations. Many companies, including many SMEs and micro-enterprises, benefit immensely from the volunteer work of open source initiatives and vice versa. The companies, in turn, participate in the maintenance and security of the software by having their employees contribute to individual volunteer projects. This participation of as many developers as possible in open source projects is in the interest of all involved and contributes to better, more secure, software. The intertwining of volunteer and commercial actors and organizations is what makes up the open source ecosystem.

In practice, however, the proposed rule would result in those employed (possibly elsewhere) ceasing their involvement in volunteer open source projects. In sum, this would lead to less rather than more secure software.

The wording in the text by the Council of the European Union already mentioned under 1) is therefore the better one here as well: "*The circumstances under which the product was developed or the way in which the development was financed should not be taken into account when determining the commercial or non-commercial nature of this activity.*"

The definition "when the main participants in free and open source projects are developers employed by commercial companies" must therefore be deleted. The text proposal by the Council of the European Union is to be given preference in the trilogue.

4) Donations - Recital 10b

The ITRE Committee text states that donations to an open source project may constitute a "commercial activity": "*Accepting donations without the intention of making a profit should not count as a commercial activity, unless such donations are made by commercial entities and are recurring in nature.*"

A large part of open source projects relies on donations (also from commercial actors), this is true for individual software projects, the large open source foundations such as the Linux Foundation, the Eclipse Foundation, the Apache Software Foundation, the Python Software Foundation, the Free Software Foundation and many more, as well as for individual volunteer developers. A stable and sustainable software project will prefer "recurring donations" for its funding, as this ensures the long-term predictability and stability of the project. The stability of open source projects is in the interest of all involved and contributes to more secure software, on which large parts of the IT economy depend.
Many European IT vendors and integrators use open source software developed by individuals and organizations that rely on recurring donations. Thus, if these were to stop working because they fall under the requirements of the CRA but cannot meet them (many of the foundations or projects do not have sufficient resources and staff to do so), the definition listed here would cut off a large portion of European IT vendors and integrators from their open source supply chain.
The definition based on recurring donations from commercial organizations must therefore be deleted.

5) Package Manager ("packet managers") - Recital 10

The text of the ITRE Committee from the EU Parliament states "*The sole act of hosting free and open-source software on open repositories does not in itself constitute making available on the market of a product with digital elements. As such, most package managers, code hosting and collaboration platforms should not be considered as distributors under the meaning of this Regulation.*"
The word "most" here means that it is completely unclear which package managers fall under the exception and which do not. This results in great legal uncertainty. The word "most" must therefore be deleted as a matter of urgency.
In the text by the Council of the European Union it reads a little better: "*A package manager, code host or collaboration platform that facilitates the development and supply of software is only considered to be a distributor if they make this software available on the market and hence supply it for distribution or use on the Union market in the course of a commercial activity*". Because here it is made clear in which concrete cases the exception should not apply.
Although both versions open up room for interpretation and thus legal uncertainties, the text proposal by the Council of the European Union with the concrete definition of when package managers do not fall under the exception should be given preference.

Request to the participants in the upcoming Trilogue

After the lead committee in the European Parliament (ITRE) and the Council of the European Union have finalized their positions in mid-July 2023, the final trilogue negotiations on the CRA are expected to begin in September 2023.

In the upcoming trilogue negotiations, the participants from the European Commission, the Council of the European Union and the European Parliament must work to ensure that the open source ecosystem and thus important parts of the European IT economy as well as Europe's digital sovereignty are adequately protected in the CRA. To this end, an exchange with representatives of the open source industry is essential.

The CRA should not hold the creator of an open source software responsible, but the "bringer into circulation" or user who offers a service with it, if money is charged for it or a business model is based on it.

During the negotiations in the European Parliament, the advisory committee for Internal Market and Consumer Protection (IMCO) had formulated a much better exception for open source software. Also the formulations in the final text by the Council of the European Union are partly better suited to protect the open source ecosystem. These should serve as a basis for the trilogue and should be given preference over the formulations of the ITRE Committee.

The European Open Source Software Business Alliance (APELL) offers its expertise in the run-up to the trilogue negotiations and is always available for an exchange as well as consultations.

About APELL:

APELL (Association Professionnelle Européenne du Logiciel Libre) is Europe’s Open Source Business Association. Founded in 2020 to bring national Open Source Software (‘OSS’) organisations together into a European network to provide them with peer support and collective marketing, as well as capacity building and policy support for public affairs, both nationally and on the EU-level.

APELL aims to increase opportunities for the members of the Association’s member organisations, and to increase value and advancement for the ultimate customers in both the public and the private sectors. At the same time, we see a real need to bring the Open Source perspective into the discussions on the shaping of Europe’s digital future.

We support the digitisation of the economy and society — but it matters how we digitise. APELL promotes a sovereign, inclusive, ethical digital market. In order to achieve this, Europe’s digital future should be based on Open.

Association Professionnelle Européenne du Logiciel Libre
Avenue des Arts 56, 4C, 1000 Brussels, Belgium
Web: www.apell.info
Contact: apell@apell.info
Transparency No. 765379449482-59