bitkom

Position Paper

Cyber Resilience Act – Bitkom Position on Open Source

17 July 2023

From Bitkom' perspective, we believe it is crucial to address the relationship between open source software and the Cyber Resilience Act. First and foremost, it is important to emphasize that open source does not fall under the framework of the Cyber Resilience Act. However, in the case of integration of open source components into commercial products the manufacturer should be responsible for due diligence. Bitkom believes that the aforementioned objective concurs with the objective of the parliament, the council and the commission. However, the current wording of the exclusion of open source software does not do justice to the objective of protecting the open source ecosystem and in turn the digital sovereignty of the European Union. Rather the current proposals burden the non-profit nature and foundations of the open source ecosystem. We therefore propose a differentiation of upstream and downstream use of open source software. The upstream use is understood as the collaboration and the release of open source software whereas downstream use is defined as the building of applications and tools based on the upstream work.

It is essential to recognize that the Cyber Resilience Act should not impede the collaborative efforts of the open-source community and commercial entities in working on open source software outside the purview of the legislation. Therefore, any liability or regulatory requirements outlined in the CRA should only be applicable to downstream use, specifically the integration of open source software in commercial products.

The collaborative development of open source software platforms plays a vital role in various digital sovereignty initiatives, including GAIA-X, Catena-X, Dataspaces, Digital Twins, and Industry 4.0. However, the implementation of the Cyber Resilience Act poses a significant threat to these initiatives. Furthermore, it jeopardizes the current and future investments made by the German government in crucial projects like federated services and Manufacturing-X. The potential impact of the CRA on these initiatives and investments cannot be underestimated, and it is essential to address these concerns to safeguard the progress and growth of the digital landscape.

Considering the modern complexities of the open source ecosystem we appreciate the possibility for the open source community to act in an advisory role to promote the development and security of software. Their expertise and insights are valuable resources that contribute to enhancing cyber resilience as well as digital sovereignty in the European Union.

We believe that a balanced approach should be adopted to protect the open source ecosystem, while also upholding the objectives of the Cyber Resilience Act. By clarifying the applicability of the CRA to downstream use and exempting non-profit

associations, we can create a conducive environment for innovation, collaboration, and cyber resilience in the digital landscape.

We therefore propose the following amendments:

Recital

(10) In order not to hamper innovation or research, free and open source software (FOSS) developed or supplied outside the course of a commercial activity should not be covered by this Regulation. Free and open source software is defined as software, which is freely accessible, usable, modifiable, and redistributable. Free and open-source software is fundamentally based on collaborative development in a shared space (aka "upstream project"), thus placing it inherently outside of the realm of a single manufacturer. Therefore, the free and open-source software in this shared space ("upstream" project) is not covered by this Regulation. However, all free and opensource software can be used in the context of a commercial activity (aka "downstream" use). Commercial activities can be differentiated in profit-oriented activities, such as specific manufacturers that bundle FOSS to monetize products and services and non-profit-oriented activities that usually foster the collaborative development of FOSS like the upstream projects themselves. This Regulation therefore applies only to such profit-oriented downstream use of free and open-source software under the purview of a specific manufacturer. The mere hosting or distribution of open-source software, participation in open-source projects, irrespective of whether a sponsorship or membership fee is paid, or technical support of a third person does neither make the person nor the open source software project a manufacturer nor qualifies as a commercial activity in the reading of this Regulation.

Article 2

Scope

1. This Regulation applies to products with digital elements whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network.

2. This Regulation does not apply to products with digital elements to which the following Union acts apply:

   (a) Regulation (EU) 2017/745;

   (b) Regulation (EU) 2017/746;

   (c) Regulation (EU) 2019/2144.

3. This Regulation does not apply to products with digital elements that have been certified in accordance with Regulation (EU) 2018/1139.

3a. This Regulation does not apply to free and open source software, unless it is integrated into a commercial product.

4. The application of this Regulation to products with digital elements covered by other Union rules laying down requirements that address all or some of the risks covered by the essential requirements set out in Annex I may be limited or excluded, where:

   (a) such limitation or exclusion is consistent with the overall regulatory framework applying to those products; and

   (b) the sectoral rules achieve the same level of protection as the one provided for by this Regulation.

   The Commission is empowered to adopt delegated acts in accordance with Article 50 to amend this Regulation specifying whether such limitation or exclusion is necessary, the concerned products and rules, as well as the scope of the limitation, if relevant.

5. This Regulation does not apply to products with digital elements developed exclusively for national security or military purposes or to products specifically designed to process classified information.

Published by
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Contact person
Simran Mann | Policy Officer Security
T 030 27576-214 | s.mann@bitkom.org

Responsible Bitkom committee
AK Informationssicherheit