



**Fecc**  
EUROPEAN ASSOCIATION OF  
CHEMICAL DISTRIBUTORS

# EU Consultation: Cyber Resilience Act

---

European Association of Chemical Distributors (Fecc)

Contact : Elias Rito, Technical & Regulatory Affairs Manager

([eri@fecc.org](mailto:eri@fecc.org))

May 2022

[www.fecc.org](http://www.fecc.org)

Fecc acknowledges the consultation on the Cyber Resilience Act ([link](#)) and welcomes the opportunity to provide input. In this context, we would like to raise the following points in this consultation:

**1. The synergy between the Cyber Resilience Act and current national initiatives should be put into perspective.** Fecc acknowledges that the aim of the proposed act is to enhance and ensure a consistently high level of cybersecurity of digital products and ancillary services. More specifically, a broad range of such products and associated services must be secured throughout their whole lifecycle proportional to the risks. Certain Member States such as Belgium, Estonia, Germany and the Netherlands already have such systems set in-place in various degrees for specific sectors. Fecc calls for the Commission to evaluate the best-practices currently being applied at a Member State level in order to avoid overlapping requirements for digital companies, most of which are start-ups, spin-off or operate at an SME level.

**2. Europe's road to digitalisation and the corresponding cybersecurity that goes along with it, goes hand-in-hand.** We have various IT company members that provide regulatory support, in line with competition and compliance rules. Our members go to extreme measures to protect their digital portfolios and client base. The digital boom we have been experiencing in Europe for the past 20 years must also be supported by cyber-attack-resilient innovations at a European level in order to further stimulate such innovations on green and digital transitions. Through this, companies would be ensured that they have the flexibility to provide B2B and B2C services whilst maintaining their long-standing compliance in terms of GDPR, cybersecurity, and competition compliance rules.

**3. The Commission shall set a system in place that safeguards legal certainty on cybersecurity for servers both within and outside the EU.** Based on a workshop held by Fecc on the topic of cybersecurity, we request the Commission to integrate the following aspects on the Cyber resilience acts:

- **Ransomware:** Detect systems being sabotaged that are not sufficiently protected
- **Corporate (CEO) fraud:** Support systems put in place that detect manipulation of communication and payment instructions
- **IoT related risks:** Provide guidance on how exploited IoT devices could be better protected by companies

As the association that also represents digital companies working with chemical, food and active pharmaceutical ingredients distributors, mainly SMEs, we believe that a cyber-attack-resilient and a sound regulatory framework go hand-in-hand. We would be happy to engage further with the Commission in the pursuit of sustainable, future-oriented solutions in this area.

To access the Fecc's response on the EU Commission's website, please click [here](#).