Open Letter:
For a successful application of the European Cybersecurity Certification Framework

Our European associations represent the **technology, engineering and manufacturing sectors** in the European Union. We provide industrial applications to a wide array of different industrial branches and across many industrial supply chains, in particular to the ICT sector. **Cybersecurity is a top priority for our industries in the B2B and B2C markets.** We already invest in the development and integration of cyber secure solutions into our industrial applications. It is of critical importance for our industry to provide our customers with safe, reliable and secure products, services and processes.

The Cybersecurity Act will have a **great impact on our industry and could be instrumental to boost Europe's global industrial competitiveness**. We call on European decision-makers to consider carefully the broad impact of this Regulation on the whole European industry and to ensure that it serves as an instrument to the European industrial strategy.

Therefore, we are greatly concerned with the ongoing political discussions and urgently call upon the European Parliament and the Council to consider three key elements of Europe's strongest industries:

1. While we welcome the inclusion of self-assessment as an alternative to third-party assessment, **its limited application to the assurance level "basic" would be detrimental to our industries**. Under the current definitions, most of our industrial applications would actually fall under the assurance level "substantial". **This puts pressure on our industries' products, services and processes that would have to undergo time-consuming and costly third-party certification,** which would severely constraint our SMEs.

2. Furthermore, to have a pragmatic and sensible approach to cybersecurity certification, it is essential to set a **transparent, flexible, inclusive and structured process**, followed by an assessment of market needs or failures **under the Framework**. Therefore, we urge the co-legislators to take into account the system of **ad-hoc consultation platforms** for the elaboration and preparation of each specific candidate schemes. **These platforms should work in close cooperation with ENISA, the Group and European Commission, with the relevant experts according to the scope of certification schemes in preparation.**

3. Lastly, Europe requires a **future-proof European certification framework for cybersecurity**. **Whether certification should be of mandatory or voluntary nature should be defined on**

a case-by-case basis, and during the process of preparing and elaborating a candidate scheme. In principle a mandatory certification system at EU level from the beginning would be to the detriment of large economic operators and European small and medium size manufacturers alike, while it is the latter that would bear the bulk of the economic burden. Furthermore, such de facto product regulation should be done through the existing and well proven (e.g. for safety) framework of the New Legislative Framework (NLF - via decision 768/2008 and 765/2008).

It is of utmost importance for the success of cybersecurity in Europe that the European Cybersecurity Certification Framework reflects these key elements. **The goal of the Cybersecurity Act is to boost Europe's cybersecurity overall and this is best achieved if a pragmatic and tailored approach to cybersecurity is guaranteed for European industries**.