ORGALIME

Our Key Messages for a Cybersafe Internet of Things

SCOPE AND DEFINITIONS

The scope of application and the **definition of ICT products and services** should clarify that these are intended **to be connected to the Internet** to be covered by certification schemes.

CERTIFICATION

Third-party certification is not always appropriate to promote cybersecurity in the market. By experience, private contracts applying to professional products (B2B) combined with the use of standards and **alternative conformity assessment procedures** often provide **more adequate**, cost-efficient and flexible answers to manufacturers, especially SMEs.

Self-declaration of conformity in particular is an established and a **well-functioning conformity assessment procedure** which should be included as an option where a minimum level of cybersecurity for certain categories of ICT products is required.

The Cybersecurity Act should ensure that future schemes **follow a risk-based approach**, depending on the context and severity of the situation, taking due consideration for the cybersecurity-by-design concept.

All future European cybersecurity compliance and certification schemes should remain of **voluntary application** as certain market factors could jeopardise the voluntary nature of future compliance and certification schemes.

The access of the European industry to the international markets is key for the success of a European digital single market. Therefore, the Cybersecurity Act should acknowledge that **international standards** could be used as the **primary reference** for the building blocks of future cybersecurity schemes.

INDUSTRY INVOLVEMENT

ENISA needs a **clear and permanent mandate** in order to improve its efficiency, and to continue to help supporting cybersecurity capacity building in the Member States.

Industry input in elaborating and preparing candidate schemes under the new governance structure is limited and **requires improvement**. The Cybersecurity Act needs to elaborate under which conditions ENISA should consult relevant stakeholders, in an open and transparent manner.

The Cybersecurity Act should take inspiration from Article 18 of the Ecodesign Directive to provide **a pragmatic solution for involving all relevant stakeholders** in the preparation of future compliance and certification schemes, including work plans, quality criteria and a stakeholder consultation forum.