Brussels, 7 February 2022

Joint industry letter on the NIS2 trilogue negotiations

Our associations, representing sectors central to Europe's digital transformation, welcome the recently launched institutional trilogue negotiations on a new Directive on measures for a high common level of cybersecurity across the Union (NIS2). To achieve the proposal's aim of tackling the limitations of the current regime and achieving a more harmonised level of cybersecurity, the final text must be clear and reliable.

Our common priority through the NIS reform should be to remove inconsistencies in resilience across Europe and sectors by ensuring a high level of harmonisation. In doing so, we must also ensure that the reform does not unduly hamper the many entities that will be subject to the new framework.

To this end, we urge co-legislators to focus on the following:

- **Scope**. **Risk-based, objective criteria** should guide Member States' identification of essential and important entities. More reassurance should be provided in the final text that only **truly critical entities** will be included, and too much flexibility for Member States should be prevented. We invite co-legislators to consider an **exclusion for SMEs** – not only micro and small businesses – unless they meet relevant criteria for criticality. The final text should also make it clear that only **activities within the EU** are in scope, as stipulated in the Parliament position. This is particularly important for manufacturing.

- **Reporting obligations**. We welcome both co-legislators' efforts to ensure that efforts go towards reporting **significant incidents**, as opposed to potential threats that would merely overburden entities and authorities alike. The Parliament, in addition, has reintroduced and expanded on criteria to determine an incident's significance. We urge the co-legislators to converge around a final **72-hour deadline for incident notification**, which will help entities focus on mitigating incidents in the crucial phases of their emergence. We also support the Parliament's position that the establishment of a **single entry point** for all notifications under NIS2 and other legislation should be mandatory for Member States.

- **Certification**. There should be no fragmentation as to if and how cybersecurity certification schemes are mandated to demonstrate compliance with NIS2. Individual Member States should be encouraging the use of certification, not mandating it. Schemes should instead only be mandated by the European Commission through **delegated acts**, and subject to the rigorous **assessment of existing schemes** stipulated under Art. 56 of the Cybersecurity Act.

- **Link with sector-specific laws**. Entities should have clarity as to the cybersecurity obligations they are subject to. We welcome the Council's inclusion of a **dedicated article** setting out conditions for equivalence of risk management and incident notification measures under sectorial laws, tasking the Commission to conduct periodical reviews.

We look forward to engaging with the European Parliament and the Council to ensure these crucial aspects are soon reflected in the final agreement.

Signatories:

- BUSINESSEUROPE
- DIGITALEUROPE
- Orgalim