BUSINESSEUROPE

POSITION PAPER

ANNEX – THE PROPOSAL FOR A CYBERSECURITY ACT – ADDITIONAL POINTS

In relation to recent co-legislator developments, BusinessEurope annexes its position paper dated 21 November 2018 to comment on a number of new elements in relation to this dossier. Nothing within the input below contradicts our original position paper. Rather, it comments on elements that did not exist or were not detailed previously due to the initial debate at that time.

A large part of this input surrounds Parliament's intention to align with **the New Legislative Framework.**[1] This is a 10-year-old flexible legislative method that enables products to gain market access. Firstly, the legislators agree mandatory societal principles needed to be adhered to before a product can be legally put on market (eg. the product is safe). Secondly, the Commission mandates CEN-CENELEC who in cooperation with stakeholders, is to design standards that use accepted industrial practices to demonstrate how their product achieves the legislators initial goal. The Commission then determines whether this is accepted as reaching its original legislative goal and if so, publishes the references to the standards in the Official Journal of the European Union (OJEU). Industries may then use the standard (or provide other demonstrable industry practices with equivalent results) in order to test the conformity of their product to gain access to the market, self-assessment can be made. Depending on the product itself, 3rd party certification of that testing could then be required in addition. In both instances, the developed standard is often used as part of the documentation that could then be required in the future if there was an incident and a reasonable request made by a market surveillance authority.

- Our aim is to ensure a voluntary but legally certain cybersecurity certification framework. In this regard we believe that it is necessary to take inspiration from the New Legislative Framework for products in developing provisions for Title III of the Cybersecurity Act that would create cybersecurity schemes. However, this first step should not go as far as to create a mandatory system.

- The Rapporteur's draft report goes in the wrong direction in this instance as it would only allow for self-certification for low-level risk. The ability to self-certify (Title II of Regulation 768/2008) for all risk levels of products and services should also be enabled. This would improve the affordability of all businesses to be able to apply these voluntary schemes.

- If various levels are going to be applied to codify these cybersecurity schemes, they should be expressed in greater detail. They should also rely upon risk alone, not assurance (which cannot be 100% guaranteed) or confidence (which is subjective). The definition of each category and the criteria that places certain products/services in those categories could be decided through comitology in order to ensure a full technical assessment is carried out in greater detail than at the political level.

- The European schemes that this framework creates should only take precedence over similar existing national schemes that are not mandatory or do not fall under the NIS Directive. Otherwise, a legal vacuum will be created when a voluntary European scheme takes place of a national mandatory one.

[1] http://www.orgalime.org/page/new-legislative-framework-nlf

- We support the initiative to create separate ad-hoc stakeholder groups for each scheme that is developed in order to give industry the opportunity to feed into the process with its technical expertise, knowledge of the market and threat landscape. However, the wording of the current proposal should be stricter. It must be mandatory that these individual stakeholder groups are set up (not ad-hoc). The make-up of these groupings is also important and must demonstrate a fair balance between users/providers.

- We do not support labelling practices or the use of a product declaration for consumers. This would send the wrong message to a consumer as it would demonstrate the product is 100% secure (impossible) but also through creating this false sense of security, the consumer does not need to act further (when we should be promoting cyber hygiene). As soon as a label is applied it also becomes obsolete and out of date with current developments in cyberspace.

* * *