Statement on the European Commission's Inception Impact Assessment "Revision of the NIS Directive" (Ares(2020)3320999)

Berlin, 12 August 2020

In its current form, the NIS Directive represents a central instrument for both the shaping and regulation of IT security in Europe. In 2017 it was once again extended by means of an Implementing Act. A large number of EU Member States have implemented the NIS Directive and also established their own regulations on its basis. The Cybersecurity Act of 2019 also draws heavily on the regulation laid out in the NIS Directive as well as on the sectoral classifications of the regulation.

With the present consultation and the associated Inception Impact Assessment, the EU Commission wants to precede the mandated evaluation of the NIS Directive and discuss various options for its further development. eco – Association of the Internet Industry sees the NIS Directive and the regulation derived from and built on it as a stringent but essentially suitable regulatory framework for the area of IT security. eco considers the following aspects to be particularly relevant for the ensuing evaluations and the present Inception Impact Assessment.

I. General remarks

The regulatory framework for IT security has gained enormous momentum over the past five years. This is understandable, given that modern information technologies and networks are increasingly being used in system-critical areas. In addition to the European regulations already mentioned, corresponding laws have also been adopted at national level: in Germany, this includes the IT Security Act of 2015, as well as the NIS Directive Implementation Act of 2017. A further IT Security Act is currently under discussion and is in the preliminary stage of the legislative process.

Against this background, it should be noted that any new regulation presents an implementation challenge for companies, given the required adjustments to operational processes and systems and the costs incurred. As such, in the interests of companies striving for legal conformity, when it comes to a dynamically evolving set of rules for IT security, there is a need to strive for rules that are consistent and comprehensible, that – side-by-side with continual technical innovations and improvements – keep the criteria and the adjustment challenges manageable, and that are carried out in reasonable cycles.

II. On the Inception Impact Assessment in detail

- **On the "Problem the initiative aims to tackle"**

The EU Commission holds the view that, while the NIS Directive has proven to be fundamentally successful with its requirement for a minimum level of harmonisation and has been widely accepted in most EU Member States, a broad range of regulations established on the basis of the NIS Directive still show a high degree of national fragmentation, with this situation calling for further harmonisation. In eco's opinion, such an endeavour is fundamentally to be welcomed. eco considers the further harmonisation of security requirements in the IT sector to be a central aspect of the further shaping of the European Digital Single Market. At the same time, eco would also like to note that national distinctions are partly attributable to the regulatory structure in other fields; for example, the legal framework for telecommunications, where a high degree of density prevails in national regulation. Here, the harmonisation should not simply be addressed with a new regulation, as this would confront companies with an overly complex adjustment challenge. Moreover, the Commission's evaluation lists "important" actors who currently fall outside of the scope of the Directive. This raises the question as to the extent to which these are actually critical fields or system-relevant actors. In eco's view, it would therefore first be necessary for the Commission to concretise its analysis before taking further regulatory steps.

- **On the "Objectives and policy options"**

The EU Commission currently visualises four different options for the further design and development of the NIS Directive.

The first option would involve maintaining the status quo and would therefore have the least impact on the current situation. It is unclear to what extent this existing status quo would encourage or challenge the respective national legislators to enact their own regulations beyond the NIS Directive and thereby further the fragmentation of the regulatory structure, a situation which, for eco, also summons up scepticism. Ultimately, it is not possible to determine with certainty the extent to which existing accompanying measures such as "best practices" would prove helpful in further harmonisation.

The second option would entail introducing further non-legislative measures to complement the existing legal framework. Similar to the first scenario, the question arises as to the extent to which these guidelines and implementing acts would harmonise with national law, or whether they would trigger duplicated regulation, and to what extent national states would feel bound by such guidelines. The underlying problem of scenario 1 could be addressed at

least in part with supplementary elaborations for developing a better common understanding of IT security. At the same time, it remains unclear what regulatory consequences would arise in the Member States with regard to the regulation of IT security.

The third option would involve a partial revision or even an expansion of the NIS Directive. eco understands this approach to mean that the existing Directive would essentially be retained, while individual parts would be revised and further specified, and where new elements of relevance to the Directive might be added. In particular, the expansion of the Directive's scope to new sectors or services which are "equally essential" would be a central aspect here. Building on the current NIS Directive, its partial adaptation would be understandable, although it is unclear to what extent the expansion of its scope would prove to actually make sense. Previous deliberations at national level have not offered a plausible justification for an expansion of the regulatory field.

The fourth option would be a completely new legislative act to replace the existing NIS Directive and create binding common rules in the area of IT security. In this case too, the consequence would be an expansion of the scope of the NIS Directive or its successor. Similar to option 3, the question arises here too of how a meaningful expansion of the NIS regulatory framework could be achieved. At the same time, the question arises concerning the extent to which a possible stricter standardisation of the legal framework would be a reaction to already existing national regulation. As already described at the outset, there are already area-specific rules in numerous sectors beyond the regulation of IT security, which would also have to be taken into account and consequently adapted.

- **On "Likely economic impacts"**

In addition to the positive aspects described in the Inception Impact Assessment, it should also be borne in mind that the continual regulatory adjustments, supplements and expansions entail the risk of a growing and diverging duplicate regulation for companies, which would confront small and medium-sized enterprises in particular with further ongoing adjustment challenges. eco essentially welcomes a solid and, if possible, Europe-wide standardised and high level of IT security. At the same time, eco would like to point out that, in order to achieve this goal, reliable, comprehensible and achievable rules should apply for companies, and that in particular the technical and organisational adjustment requirement should remain manageable for these companies. This should be taken into account in particular in the further development of reporting and notification obligations.

III. Summary and assessment

With a revision of the NIS Directive in a dynamic regulatory environment, the EU Commission has set itself the ambitious goal of significantly expanding the existing NIS Directive – which has been rated as successful in principle – and of standardising its application in the EU Member States to a greater extent. eco welcomes the Commission's goal and considers it worthy of support in principle. At the same time, eco emphasises that companies have to take not only European but also the respective national legal situation into account when making any adjustments. With regard to a possible expansion of the existing NIS regime to encompass new sectors and fields, the question arises as to how these are to be shaped and to what extent the rules for these sectors would be transparent and proportionate. In this context, further legal questions must also be taken into account, such as the impact on, and compatibility with, freedom of information and freedom of the press. In eco's opinion, this must be taken into account as a matter of urgency in the further development of the NIS Directive framework. A successful further development of IT security regulation would certainly benefit from further harmonisation of regulations within the framework of the Digital Single Market.

About eco:

With over 1,100 member companies, eco is the largest Internet industry association in Europe. Since 1995 eco has played a decisive role in shaping the Internet, fostering new technologies, forming framework conditions, and representing the interests of members in politics and international committees. eco's key topics are the reliability and strengthening of digital infrastructure, IT security, and trust, ethics, and self-regulation. That is why eco advocates for a free, technologically-neutral, and high-performance Internet.