POSITION PAPER

on the Proposal by the European Commission for a Regulation of the European Parliament and of the Council on ENISA, the 'EU Cybersecurity Agency', and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ('Cybersecurity Act')

Brussels/Berlin, 18 January 2018

To pursue its ambitious goal of creating a digital single market for Europe, the European Commission has already instituted several measures. The topic of IT security has also been broached as part of these developments. Thus far, this has entailed its being dealt with at European level primarily through legislation (the NIS Directive), through proactive information policy and development policy within the framework of research programs, and through awareness training and networking of national actors by the EU Cybersecurity Agency ENISA.

In keeping with the Commission's wishes, the Agency is now to be assigned an extended mandate, and will be able to better coordinate options for responding to security incidents. It is also intended that ENISA will intensify its activities in the area of certification and standardization for IT security.

In order to do justice to the new tasks, a new mandate for ENISA is necessary to now establish the Agency as a permanent European institution.

In addition, the EU Commission wants to harmonize the landscape of cybersecurity certification in Europe and to create a unified framework for a European cybersecurity certificate involving different gradations, with this framework to replace the various national measures.

eco is accompanying developments in the field of IT security at national and European level with the aim of shaping IT security and trustworthiness in a dynamic and innovative environment. From eco's perspective, the following aspects are particularly significant:

1. Measures for a European IT Security Agency

▪ IT Security – a commitment for all stakeholders

Ensuring IT security is a challenge for all stakeholders – users, manufacturers, and the State. The Regulation attaches a particularly high level of importance to the role of manufacturers in endeavouring to close security vulnerabilities and in ensuring that their products are designed in a manner which is both responsible and as secure as possible. However, it remains largely silent on the theme of how governments and Member States should behave. IT security for users can only really be provided if these stakeholders also take up this challenge. However, current discussions in several EU Member States and at the level of the Commission about statemandated backdoors or access to encrypted or secured data show that there are also moves afoot which, if realized, would lead to a systematic and significant undermining of the IT security of products and services. Here, government agencies must assume responsibility and report known vulnerabilities immediately so that companies can quickly close them.

- **Stringent regulatory structure and a clear mandate for ENISA**

The EU Commission's analyses acknowledge that many Member States have already taken organizational measures in the field of cybersecurity and have established rules for reporting IT security incidents. The revision of the European institutional framework also represents a challenge for these already nationally established institutions. Avoiding any overlapping or duplication of responsibilities, reporting obligations, or competencies as a result of an extension of the ENISA mandate is of paramount importance. For the purpose of efficiently eliminating disruptions or preventing attacks, all of these factors should be clearly regulated and should not burden companies with additional bureaucracy.

- **Collaborative approach to IT security**

The EU Commission proposal recognizes that IT security cannot be designed without the suppliers of products and services. With the planned ISACs, it is also intended that institutional opportunities be provided for the inclusion of digital service providers. In order to achieve unqualified success in improving IT security, it is essential that this collaborative approach be consistently and comprehensively implemented. It is only in so doing that trust-based and consequently successful cooperation for greater IT security can be realized.

- **Making quality visible – creating transparent and practicable supports**

As a means of presenting and structuring cybersecurity, IT seals of approval offer mixed benefits. While they can provide users in general with an overview of certain measures used to secure the systems and thus supply orientation support, when it comes to the area of IT security in particular, a more profound understanding of the underlying problems is also required. The detection of security vulnerabilities in certified products could undermine confidence in the seal and in modern information technology in general – a situation that needs to be critically examined.

In considering possible approaches to certification or a seal, technical properties should not be the only factors taken into account as a testing dimension; rather, the risk management relevant to the application – i.e. how detected security vulnerabilities and communication with consumers are handled – should also be considered.

2. On the individual regulations:

Based on these provisions, eco considers the following aspects to merit further consideration in the proposed Regulation:

- **On Article 7: Tasks relating to operational cooperation at Union level**

The Article specifies measures for the work of ENISA as a Security Agency. Apart from supporting national and European CSIRTs, this also includes sharing of information and reports. It is of the utmost importance that the knowledge accumulated by ENISA is not used by the Agency itself to carry out or prepare cyberattacks, or to facilitate cyberattacks by national security authorities. This could defeat ENISA's efforts and destroy companies' confidence in the institutional framework of ENISA. Article 7 (2) lit. c) is intended to resolve any ambiguity. The "Good Faith" referred to in Recital 21 may have an appellative effect here, but under certain circumstances, it may also prove to be insufficient.

- **On Article 20: Permanent Stakeholders' Group**

The Permanent Stakeholders' Group planned within the framework of the ENISA provision represents a collaborative approach to IT security regulation, an approach which eco welcomes. What would also be desirable here would be a stronger emphasis on open and expert participation in the Permanent Stakeholders' Group. Recital 30 of the Commission's proposal envisages this group being principally comprised of other authorities, with these tending to make demands on IT security rather than proactively shaping it. Recital 44 also focuses first and foremost on dialog with users and customers. More important tasks at this juncture are the proposed collaboration in the ENISA annual program and the critical appraisal of the Agency's work derived from Article 20 (5).

- **On Article 43: European Cybersecurity Schemes**

The proposed European framework for cybersecurity certificates is not deemed to be practicable in its proposed form. Individual products or their elements are too differentiated, so that products and services are often difficult to evaluate or classify independently of others. In addition, such a certification framework is often only conditionally – or not at all – suitable for correctly recording organizational or human factors. There is also no hard-and-fast clarification concerning the degree to which such a certification framework interrelates with other efforts, such as in the field of standardization or with privately organized quality seals. A more constructive aspect relates to the consideration of protection profiles, which are to be scrutinized based on their level of criticality and which will form the basis for the discussion of an EU-wide transparent certification framework. Moving beyond a mere technical snapshot, security-by-design approaches for the lifecycle of a product could, for example, be used to address the closure of security vulnerabilities.

- **On Article 44: Preparation and adoption of a European Cybersecurity Certification Scheme**

The prescribed procedure here would involve the submission of the developed framework for cybersecurity certificates to the Commission, which can then also adopt relevant implementing acts. This implies that the proposed framework will go far beyond being just a quality seal or recommendation. Here, interrelationships with existing quality seals such as the CE marking must be considered. More light needs to be shed on the fact that the implementing acts may, under certain circumstances, entail legally binding obligations up to and including product liability. Aside from the formal and unsatisfactory parliamentary control of the implementing acts, the aim of these acts is so vaguely formulated that it is not possible to assess the potential impact on the Internet industry. A hastily-formulated regulation cannot be desirable in terms of a stringent IT security policy. There would be too great a risk that the allegedly secure standards, enforced by a legal decree, would prove to be compromised, thereby damaging the entire certification framework.

- **On Article 45: Security objectives of European Cybersecurity Certification Schemes**

The proposed objectives for the framework for EU cybersecurity certificates may in themselves be understandable and plausible. At the same time, however, the question is also raised here as to what extent they will also serve to counteract existing regulations – and possibly laws. For example, the protection of data as required in Art. 45 (a) and (b) may conflict with the requirements of the EU General Data Protection Regulation (GDPR), which envisages its own seals.

Consequently, the verifiability of data access in Art. 45 (c), (d), and (e) conflicts with the GDPR and the ePrivacy Regulation.

Furthermore, it is not clear for whom this access should be recorded and to what extent a binding provision for all IT systems is appropriate.

In practice, it will be difficult to control for ‘exemption from known backdoors’ and for actuality (Art. 45 (g)). In this respect, establishing concrete technical requirements for products is regarded by eco as being counterproductive.

- **On Article 46: Assurance levels of European cybersecurity certification schemes**

The stipulation of security levels in the framework for IT security certificates demonstrates that neither the topic nor the underlying problems have been correctly grasped. Generalized statements about the security of networked systems require careful analysis – an analysis which also takes possible risks into account. The scheme outlined here does not consider these aspects.

What is also unclear is the extent to which the draft version chosen here – which the text does not see as conclusive (cf. Art. 46 (1)) – is appropriate and whether it preempts the work of ENISA and the European Cybersecurity Certification Group. In order to enable a reasonable differentiation to be made, connected devices should be evaluated with regard to their criticality.

- **On Article 47: Elements of European cybersecurity certification schemes**

As with Article 46, the question also arises here as to whether a statutory stipulation of the components of a certificate for cybersecurity preempts the work of the bodies designated for this purpose. Whether the approach adopted by the Commission as a whole makes sense is also called into question with this Article. This is strikingly underlined in Articles 47 (3) and (4), where corresponding certified products are presumed to comply with the law.

The amalgamation of cybersecurity with surveillance, as envisaged in Article 47 (g), is highly problematic and is categorically rejected by eco. A fundamental tension exists between cybersecurity and surveillance. To oblige companies to now report on compliance with surveillance measures would merely instil a lack of trust in the security of digital services and products.

Compounding this situation is the fact that Article 47 (1) (m) alludes to the possibility of consequences of deviating from the prescribed standards. This clearly underlines the Commission's intention to reinforce the seal with sanctions.

Putting aside the question of whether regulation is necessary, the foundations of a certification scheme should be based on widely accepted minimum standards in order to achieve the broadest possible market penetration.

- **On Article 48: Cybersecurity Certification**

The Article makes it clear that certificates may only be issued under the European framework for cybersecurity certificates in accordance with very strict conditions (Article 48 (4)). In concrete terms, this creates the risk that there may be bottlenecks in the issuing of certificates during implementation. These would have to be issued for a multitude of devices and products. The re-certification problem – the fact that a new certificate could theoretically become necessary by updating or adapting software functions in particular – is not covered by this aspect. A security-by-design approach could be discussed as a possible solution to this challenge and as part of a certification framework, as this is the only way to address challenges along the product lifecycle.

In addition, it can be postulated that the award of such a certificate should not be obligatory (Article 48 (2)), but this creates an unclear interplay with the liability issues raised in Article 47. In principle, and especially from the consumer's point of view, a possible certification framework should be equipped with a high degree of comprehensibility.

- **On Article 49: National Cybersecurity Certification Schemes and Certificates**

The provision to dispense with the awarding of national cybersecurity certificates or the rules for these is intended to clarify that the European framework for cybersecurity certificates will act as a consolidator. This may make sense in the context of a European digital single market. However, the extent to which private seals and their statutory support will also be affected remains unclear. This also applies to private seals offered throughout Europe. In this case, it is particularly evident that the framework for European cybersecurity certificates is not yet strictly defined and, that being the case, the pressure towards rapid market consolidation seems rash. It would be more advisable to open up the certification market more widely and thus ensure a rigorous transition from the national to the European certification framework. This should not affect the relationship between private initiatives that emphasize certain qualities of products. Here too, one option would be to consider protection outlines.

- **On Article 50: National Certification Supervisory Authorities**

The provision concerning national supervisory authorities for cybersecurity certificates adopts a structurally comprehensible approach that would also allow national authorities to delegate certain tasks. This also gives companies that have already acquired a security certificate or seal at national level the opportunity to work further with existing contacts.

At the same time, in view of existing experience in the implementation of the NIS Directive, it should be kept in mind that the respective EU Member States may also, under certain conditions, be able to assume responsibilities collaboratively.

- **On Article 53: European Cybersecurity Certification Group**

The fact that the European Cybersecurity Certification Group is composed of representatives of the respective national supervisory authorities is understandable. However, what is lacking in this body – a body which is central to the development of the certification framework – is a consultation mechanism. Especially in the context of this framework, which is so central to cybersecurity, a wide-ranging consultation would be desirable for the purposes of successful design and for delivering users with a product which is verifiable throughout the EU.

About eco

eco – Association of the Internet Industry fosters all companies that create economic value with or on the Internet and represents their interests. The association currently represents more than 1,000 member companies.

These include, among others, ISPs (Internet Service Providers), carriers, hardware and software suppliers, content and service providers, and communication companies. eco is the largest national Internet Service Provider association in Europe.