WE ARE SHAPING THE INTERNET.
YESTERDAY.TODAY.BEYOND TOMORROW.

eco

Position Paper on the Commission's draft Directive "on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148"

Berlin, 4 February 2021

With the NIS Directive from 2016 and the EU Cybersecurity Act from 2019, the European Union created the framework for the legal and institutional design of IT security measures for the EU and its Member States. With regard to the NIS Directive, an expedited review at the beginning of 2020 announced the prospect of a new regulation. With the now presented draft Directive "on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148", the Commission has acted on this announcement and launched a successor directive (hereinafter referred to as NIS-2).

The draft Directive now on the table is intended to replace the former NIS Directive and adapt its regulatory field to meet new challenges. eco commends the efforts of the EU Commission to improve and further harmonise IT security in Europe, and suggests that the Commission's work in this field should take the successes of the former NIS Directive into account.

eco sees the Directive as an appropriate framework for shaping the regulation of IT security in Europe and also expresses the hope that it will strengthen the European Digital Single Market. eco appreciates that the regulatory framework envisaged by NIS-2 is intended to be robust and that, in essential aspects, it seeks to embed the experience which has been gained from the previous NIS Directive. At the same time, eco would like to offer additional remarks on some aspects with a view to achieving a stronger orientation towards the Digital Single Market. Finally, from eco's point of view, the role and significance of what are termed as "important entities" should be further defined and concretised in order to enable a more constructive classification of critical infrastructures.

Regarding the present draft Directive, eco would like to make some initial remarks, as follows.

I. General remarks:

- **Affected group of "important entities"**

The NIS-2 Directive sets forth a regulatory field consisting of "essential" and "important" entities. The former group is strongly linked to the regulatory framework of critical infrastructures (CI). With the "important entities", on the

other hand, the regulatory field is extended to further companies. A key success factor for the future design of IT security will revolve around the question of how these “important” entities are regulated. The Commission’s draft envisages an ex-post supervisory regime for this and outlines sectors and companies to be classified as “important entities”. It remains unclear, however, how the ex-post supervision for “important entities” is to be set up and to what extent the conditions, targets and thresholds differ from those of “essential entities” in concrete terms. From the point of view of the Internet industry, greater clarity is needed here in order to better differentiate between the regulation of “essential” and “important” entities.

- **Ensuring IT security in supply chains**

In light of the roll-out of new mobile networks with the 5G standard, a topic under discussion in both the Member States and at European level concerns how IT security can be secured in supply chains. Of additional importance is the question of which hardware is used in IT systems and to what extent technologies are particularly exposed to attacks. While the specific design of the corresponding measures is the responsibility of the Member States, eco believes that, in the interest of a Digital Single Market, working towards greater harmonisation of the various national regulations would make sense and be worthy of support. This idea is partly taken up in NIS-2, but should be supported in particular by the NIS Cooperation Group and through stronger systems of norming and standardisation at European and international level.

- **Conditions for domain name systems must be of a proportionate scale**

From eco’s point of view, the conditions that NIS-2 envisages for registrars and registries are too stringent. The domain sector is essentially a mass market business, so that the constant and precise identification and verification of domain holders would impose an enormous bureaucratic and financial burden on registrars and registries, and would ultimately also have an impact on users. This would basically only be offset by limited benefits, meaning that the proportionality of the associated NIS-2 measures should be critically reviewed. In the past, eco has advocated that, where necessary, identification should be carried out on the basis of the payments made and the stored payment data, and that the corresponding information should be retrieved in this way. Such a “follow-the-payments” approach would be just as effective, less invasive, and more manageable for the companies concerned.

II. On the articles in detail

On Article 2: Scope

In the NIS-2 draft, Article 2 (2) also applies to “public electronic communications networks or publicly available electronic communications services”. This essentially corresponds to the scope of application of Article 40 of the European Electronic Communications Code (EECC). What is unclear, however, is how the two regulations interrelate with each other. If such measures are not reciprocally followed up in the EECC in an equally consistent manner, eco sees the risk of double regulatory action. Here, clarification would be desirable, meaning that the measures of the EECC should be revoked and integrated into the NIS-2 Directive, or that companies regulated via the EECC should become exempt from the NIS-2 Directive. Given that this is not currently envisioned, eco sees a need for remedial action.

In addition, the Article 2 proposal raises the question of the extent to which the manufacturers of hardware and software for the operators of critical infrastructures are to be included in the NIS-2 measures. Currently, the draft NIS-2 envisages that telecommunications companies in particular should be solely responsible for the secure operation of their infrastructures and supply chains, and creates a proviso for their further regulation (cf. Article 18 (3) and Article 19). Here, the inclusion of suppliers and developers in the measures would be welcome – also in the sense of an appropriate distribution of responsibilities for IT security – so that, in complying with the corresponding measures, the operators of essential and important entities would not have to bear the entire risk of contractual and economic drawbacks.

Furthermore, NIS-2 draws a distinction between digital service providers and data centres. The Commission has thus taken heed of the criticism of how the term cloud service providers was used in the former NIS Directive, where it was often defined too imprecisely. eco welcomes this clarification, but at the same time would like to emphasise that the respective measures for digital service providers and data centres should not be in conflict with each other. In order to avoid double regulation, they should be coordinated and interlock with each other.

On Article 3: Minimum harmonisation

As was also the case with the previous regulation, the Commission has chosen the path of a directive, a choice which can be understood in view of the legislative requirements of the Union. The fact that the Directive is harmonised and thus sets a Europe-wide minimum standard is to be commended. It would also be desirable if the Commission and ENISA worked towards implementing and establishing a regulatory regime throughout Europe that is as uniform as possible. In this light, eco recommends an examination of which aspects of the NIS-2 Directive proposal could be implemented within the framework of a regulation, so that

a full harmonisation of IT security regulation could be realised at least for these areas.

On Article 5: National cybersecurity strategy

eco supports the Commission's approach of requiring Member States to develop national cybersecurity strategies on the basis of the Directive. With the aid of the NIS-2 Directive specifications, such strategies could achieve goals which are both concrete and capable of being put in motion. These strategies would be set to not only evince potential from technical, legal and institutional development perspectives, but also to make possible divergences in the respective national regulatory approaches visible at an early stage. In parallel to this, national cybersecurity strategies could also address other aspects, such as securing supply chains. In this context, eco would like to point out that corresponding national initiatives could run the risk of resulting in a strong fragmentation of the IT market in Europe. Aspects that could amount to a stronger fragmentation of the Single Market should be removed from the Directive. Instead, increased cooperation and harmonisation should be sought through the NIS Cooperation Group and the European Cyber Security Agency. Although these bodies cannot then make binding specifications, they would generate a generic standardising effect that all Member States would take on board.

On Article 6: Coordinated vulnerability disclosure and a European vulnerability registry

eco welcomes both the approach of introducing a structured and cross-border mechanism for reporting security vulnerabilities, and that of including manufacturers of information and communication technology in the reporting structures, as well as the companies affected by security incidents. eco endorses the Commission's approach and sees it as an opportunity to significantly improve the existing reporting structures. At the same time, however, care should be taken to ensure that the reporting processes are as efficient as possible. In this way, it would be possible to enable companies to act quickly and efficiently on the notifications received and not to be held back by excessive information obligations. In this regard, the scope of the notifications should also be clearly defined and specified.

On Article 10: Requirements and tasks of CSIRTs

The possibility for CSIRTs (Computer Security Incident Response Teams) to undertake proactive measures in scanning networks and technologies, as set out in the draft NIS-2, Article 10 (2), Point e, is very unspecific in its present

form, since any entity would appear to be entitled to demand corresponding measures from the CSIRTs. Network and port scans constitute far-reaching encroachments into IT systems and networks, which could result in harmful effects, and should therefore only be allowed to be carried out by or on behalf of the respective network operators or entities concerned. In eco's opinion, the far-reaching degree of encroachment and the effects on the infrastructures mean that the authority and the scope for the measures and the authority of the CSIRT must be clearly and conclusively defined and determined in this instance.

On Article 17: Governance

eco welcomes the efforts of the EU Commission to strive for a harmonised implementation of NIS-2. What is also laudable is the fact that, aside from the essential entities (CI), what are referred to as "important entities" are also to be more strongly supervised. Against this background, eco assesses the intended measures on governance as fundamentally positive. However, eco sees the requirements for the specific "trainings" of management members of the related entities as a disproportionate measure that would generate administrative effort without being offset by any distinguishable added value. It can basically be assumed that essential and important entities employ and have specialised teams available for securing their IT systems, which implement all individually required specific measures. In this context, obligations that go beyond this and the proposed "trainings for management" are seen to serve no purpose.

On Article 18: Cybersecurity risk management measures

In order to be able to effectively regulate and monitor cybersecurity, the competent national authorities must take appropriate and proportionate measures. In this respect, eco considers the measures and requirements in Article 18 to be fundamentally appropriate. At the same time, it is important to bear in mind that the respective measures must meet the different requirements for essential and important entities. However, here the standards set in the draft Directive do not appear to be sufficiently differentiated. In addition, eco would like to point out that, in order to avoid fragmentation with regard to the Digital Single Market, measures on supply chains should where possible generally be addressed at the European level.

With regard to the measures on the use of encryption, it should be added that these must also involve the manufacturers of end devices and software and not only the essential and important entities, since end-to-end encryption in particular can only be realised effectively with manufacturers' support.

On Article 19: EU coordinated risk assessments of critical supply chains

Coordinated risk assessment of supply chains is, in the view of eco, an important element for shaping IT security in Europe and takes the Digital Single Market appropriately into account. In this context, eco positively regards the explicit reference to coordinated regulation as a possibility at European level. Nonetheless, eco contends that it is imperative to assign even greater importance to the coordinated approach proposed by the measure.

On Article 20: Reporting obligations

eco regards notification procedures and the exchange of information on security vulnerabilities as an important contribution to ensuring IT security. However, the obligation to notify users of any disruptions in services is problematic in the proposed form, as the possibilities to contain and track associated attacks are restricted and undermined by a corresponding notification obligation. eco advocates for making the notification obligation to users voluntary. Mandatory notification should only be provided for in the case of a possible data leak or the necessity of user intervention (e.g., a password change).

Furthermore, in eco's opinion, the notification requirements set out in Article 20 for essential and important entities are not practicable. The multi-stage notification procedure established on the basis of Article 20 (4) would be impracticable, involve considerable administrative effort, and would therefore unnecessarily tie up resources that could be better used to deal with the security incident. The proposed time limit of 24 hours for the initial notification is too rigid and not conducive to the actual management of the IT security incident. What would make sense is the application of the reporting system established in the existing NIS Directive. Under this system, reports should be made immediately (without culpable delay). In this way, a proportionate and at the same time functioning reporting regime could be established and the number of regularly updated intermediate reports could be significantly reduced.

On Article 21: Use of European cybersecurity certification schemes

Cybersecurity certification schemes can make a useful contribution to improving IT security by providing users with a structured overview of the market. However, when developing such certification schemes, it should be ensured that they are primarily aimed at conformity with certain security requirements and compliance with procedures and standards, so as not to

undermine their credibility and counteract the added value offered by the corresponding certification structures.

On Article 23: Databases of domain names and registration data

The obligation to provide regularly updated information about the operators of domains for registrars and registries is excessive in eco's view and presents a considerable administrative and financial burden for the companies concerned. What is also uncertain is to what extent this measure would actually improve the security of IT systems, e.g., if a domain is redirected or a website stored on the domain is hacked. In this light, eco considers this obligation to be of a disproportionate scale and calls on the lawmaker to once again critically re-assess the requirements for registrars and registries of domains and to scrutinise their added value when it comes to security.

On Article 24: Jurisdiction and territoriality

The clarification on the regulation of the companies named in Article 24 (1) is to be welcomed in theory. However, eco also sees the need to clarify the extent to which the measures are to be applied, in particular when it comes to the regulation of cloud services which are offered across Europe. As a matter of priority, these should be prevented from being subject to unclear supervisory structures. Accordingly, eco would welcome further clarification concerning which of the following is decisive: the main establishment of a corporation or the main establishment for the legal entity of a corporation that offers the related service.

On Article 25: Registry for essential and important entities

The measures envisaged in Article 25 for the registration of essential and important entities would impose a notification obligation on the companies and entities concerned. At the same time, the national supervisory authorities would also be obliged to maintain corresponding contacts with contact persons. In the Article 25 measures, eco identifies a risk of a double registration obligation, and rejects this as being overly bureaucratic. Instead, it would make more sense if the registration of essential and important entities could take place either in the respective Member States or directly with ENISA and then be passed on to the other corresponding entity in each case.

On Article 29: Supervision and enforcement for essential entities

eco regards the options for supervision of essential entity providers as set out in Article 29 as too far-reaching. The right for authorities to receive corresponding information from operators of essential entities must be linked to sufficient conditions for their further use, as this could often involve operational information as well as confidential business information. This being the case, eco believes that it is necessary that the related obligations for essential entity providers go hand in hand with corresponding obligations for the authorities making the requests.

Moreover, the requirements from Article 29 (2), Points c and d are particularly far-reaching and incisive; in conjunction with Article 10, these could also incite simulated or actual attacks on IT systems of the associated entities, which could have a long-term effect on the operation of the entity and also cause severe economic damage. Given these risks, the associated measures must be urgently restricted and limited to what is absolutely necessary.

Furthermore, the measures contained in Article 29 (5) to sanction individuals from essential and important entities are of a disproportionate nature. The proposed measures clearly exceed the usual degree of organisational liability and encroach on the right to free professional practice. In eco's opinion, these measures are not compatible with the requirements of Article 15 of the European Charter of Fundamental Rights.

On Article 30: Supervision and enforcement for important entities

eco endorses the approach chosen by the Commission to establish ex-post supervision for important entities, believing that this can serve as the basis for a comprehensible and proportionate regulation of IT security for central parties below the CI threshold. At the same time, eco sees a challenge in differentiating the requirements for important entities appropriately from those for critical infrastructures. As such, further elaboration and a concretisation on the supervision of important entities and the regulatory framework envisaged for them would be welcome.

On Article 31: General conditions for imposing administrative fines on essential and important entities

In eco's opinion, the Directive's penalty framework of 2 percent of the annual turnover or 10 million Euro is far too high. This framework is based on the penalty rules of the General Data Protection Regulation, which are designed on the assumption of a significant encroachment into the privacy of citizens. While this can theoretically also occur in the case of an IT security incident, it would not necessarily be the case. The extent to which the penalties outlined

here also cumulate with possible further penalties for data protection violations remains unclear, but can be assumed. eco accordingly advocates choosing a more suitable and significantly lower approach for the penalties.

On Article 32: Infringements entailing a personal data breach

The notification obligation for data loss with an impact on the General Data Protection Regulation (GDPR) is a plan that can be understood. In the opinion of the eco, however, this could give rise to the problem that, due to the discrepancy between data protection supervision and IT security supervision, the reporting obligations and reporting channels would often be duplicated. Therefore, making the number of notifications as efficient and effective as possible in the event of a disclosed security problem would be welcome. This would ensure that, in a critical and difficult situation, resources could be used efficiently and effectively to resolve the security incident. eco is therefore in favour of designing the reporting channels and reporting chains efficiently and effectively, preventing duplicate reports from the outset, and pooling responsibilities.

Conclusion:

The draft of the European Commission's NIS-2 Directive essentially presents a meaningful and solid regulatory structure that builds on existing structures and procedures. eco assesses this as positive. It is also deemed to be reasonable that numerous aspects touched upon in the Directive are reserved for national legislation and cannot be regulated by European legislation without further action. Nevertheless, eco would like to point out that a more stringent focus on the Digital Single Market must become a central element of the NIS-2 Directive if it is ultimately to be successful. Otherwise, the planned extension of the scope of application to "important entities" would run the risk of further fragmentation and growing confusion for the European Internet industry. eco therefore advocates strengthening corresponding efforts to institutionalise IT security regulation at the European level. In doing so, care must be taken to fully exploit the potentials and capacities of existing entities, such as the NIS Cooperation Group or equivalent regulatory and standardisation bodies. This is the only way to avoid an overly complex institutional structure. In addition, care must also be taken to ensure that the expansion of the scope of NIS-2 does not result in duplication or multiple regulation. Accordingly, special attention should be paid to the telecommunications sector, which is already regulated by special legislation. The planned extensive powers for national supervisory authorities and associated CSIRTs, which would imply far-reaching encroachments in infrastructures and IT systems and which could impair their functionality, must be critically scrutinised and subjected to a review in the further legislative process. In addition, the compatibility of the NIS-2 measures and

the associated potential encroachments into compatibility with the EU Charter of Fundamental Rights should be critically examined and given a legally secure form.

About eco

With more than 1,100 member companies, eco is the largest Internet industry association in Europe. Since 1995 eco has been instrumental in shaping the Internet, fostering new technologies, forming framework conditions, and representing the interests of members in politics and international committees. The focal points of the association are the reliability and strengthening of digital infrastructure, IT security, trust, and ethically-oriented digitalization. That is why eco advocates for a free, technology-neutral, and high-performance Internet.