May 2021

EurEau Comments on the Commission proposal for the revision of the NIS-Directive; (EU)2016/1148 (Security of Network and Information Systems)

1. Key statements

The European Commission presented the legislative proposal for the NIS Directive 2.0 on 16 December 2020. This revision of the 2016 Directive aims to adapt the legal framework to technological progress and the evolving threat landscape by means of new uniform EU cyber-security standards.

EurEau agrees with the Commission that the applicable legal framework must be able to cope with the dynamically evolving risk landscape. The trustful and binding cooperation between the responsible authorities and affected entities within the framework of national industry working groups and for resolving incidents plays a central role.

However, the current directive is just being implemented at national level. There is little or no experience as to how it functions in practice. The revision is therefore premature. The European Commission should **focus on effective implementation of the current framework** in order to achieve a harmonised level of security in all Member States.

If the European legislators decide to proceed with the revision, they should focus on the further **development of a coherent and streamlined regulatory framework** for the security of network and information systems, without imposing additional and excessive burdens on industry.

At the same time, any duplication of legislation and inconsistencies with existing sector-specific and digital EU law should be avoided. The revision of the Directive should lead to a **further strengthening of the preventive approach**. This includes all aspects of detection and recovery by providing more and more detailed **information on risks and incidents in the Member States, from national competent authorities to operators of essential services**.

Furthermore, the revision should lead to an enhanced strategic **EU-level dialogue on cyber risks and threats.** This would provide additional justification for EU action.

Rue du Luxembourg 47-51, 1050 Brussels, Belgium
00 3 (0)2 7064080 - secretariat@eureau.org – www.eureau.org

2. EurEau proposals for amendments

In line with the above, EurEau wishes to put forward the following amendments:

Article 2 + Annex 1: Scope of the Directive

EurEau is strongly opposed to the proposed scope of the directive. If maintained, it would put a **disproportionate burden** on many water operators. The **reference to the EU SME Definition (2003/361/EC) should be deleted.**

In its proposal, the Commission extends the definitions and criteria determining the scope of the Directive to ensure comprehensive coverage of the sectors and services that are essential in the internal market for basic social and economic activities. Only micro and small enterprises as defined in Recommendation 2003/361/EC (EU SME Definition) are exempted, provided a "potential disruption" would not have "an impact on public safety, public security or public health (art. 2 (d)). This rather vague clause means that, in practice, even the smallest entities will be covered.

The implementation of this Directive is complex and expensive, and may lead to **disproportionate costs for micro, small and medium-sized water operators** compared to the risks it aims to address.

Selection criteria must be risk-based

The overwhelming share of drinking and waste water operators are small local entities with two to three employees. The average number of employees is around eight. There are only very few interconnections, even between neighbouring municipalities. Hence, in the event of an incident, it would generally remain limited to a small area.

The number of employees and the turnover of entities, as used in Commission Recommendation 2003/361/EC, **are not suitable criteria for deciding on the criticality of an entity**. Rather, Member States should identify essential entities based on a **risk assessmen**t using criteria determining their **systemic relevance** They should include the **number of people that could potentially be affected by an incident**, the **risks of spill-over effects to other Member States/regions** and possible **interdependencies** with other critical sectors.

Based on such a risk assessment, **micro-enterprises and SMEs should not be considered essential entities in the sense of this Directive**, unless Member Sates identify the need for a specific entity to be included.

Ownership structure is irrelevant

Many water operators are organised as public companies or departments of municipalities. The SME definition in Recommendation 2003/361/EC excludes enterprises if at least 25% of the shares are controlled by a state body or public corporation. According to this logic, all small water operators that are partially/predominantly (> 25%) owned by municipalities would be covered by the Directive's scope.

Any reference to the ownership structure of essential entities should be removed from the Directive. As outlined above, entities should be selected following a risk assessment approach.

Inclusion of the waste water sector

Regulations regarding waste water management differ between EurEau member countries. In some, waste water is defined as a critical infrastructure, in others, this is not the case.

EurEau recommends that the decision to include waste water operators in the scope should be left with Member States. If a Member State decides to include waste water operators in the list of essential entities, the NIS Directive should apply.

Article 20: Information sharing & reporting obligations related to cybersecurity incidents

EurEau supports the legal obligation to report significant cybersecurity incidents. However, reporting obligations should continue to be limited to significant **cybersecurity incidents with supra-regional, national, or** European significance. Multiple and competing reporting obligations and responsibilities must be avoided. Notification deadlines must be reasonable.

The requirement of paragraph 20.2 to report "near misses", is not supported. This would lead to a disproportionate reporting burden.

Annexes 1 and 2: Digital service providers and manufacturers / solution providers

EurEau welcomes the **equal treatment of water operators and providers of digital infrastructure as essential institutions**.

Manufacturers and solution providers of ICT products, services and processes should make an increased contribution to the protection of critical infrastructures in the future. To this end, the product liability regulations should be expanded to include aspects of IT security. **Security by design should be enforced** and continuous improvement should be encouraged.

Articles 18, 19: Risk Management Measures and coordinated Risk Assessments of Supply Chains

EurEau agrees with the Commission's observation that in times of globally interconnected production methods and international supply chains, cyber security risks to the IT systems of essential entities are increasingly emerging along critical supply chains. The Solar-Winds case highlights the worrying threat of attacks across supply chains.

The current regulatory framework shows gaps in addressing this issue and should henceforth ensure the pooling of intelligence from national competent authorities for further analysis of cyber threat scenarios from a strategic and EU perspective. **EurEau therefore suggests that the provisions of article 19 (1) become a requirement ("shall" instead of "may") and that it be stipulated that the knowledge gained, e.g. on attack strategies, statistical information and other sources and types of**

information, be made available to the operators of essential and important services in a timely, up-to-date and regular manner. Furthermore, a **structured dialogue on the treatment of potential, identified risks along critical supply chains** should be conducted with all relevant stakeholders in order to strengthen the technological sovereignty of the EU in the long term.

Consequently, EurEau welcomes the Commission's proposal to mandate the NIS Cooperation Group under Article 19 to conduct risk assessments of supply chains in a structured and coordinated manner to identify critical ICT services, systems or products and relevant threats and vulnerabilities for each sector.

- In addition, the Commission proposes two further approaches to address cybersecurity risks along supply chains: Member States shall, as part of the national cybersecurity strategy, present a cybersecurity supply chain approach for ICT products and services used by essential and important entities for the provision of their services.
- As part of the risk management measures, Article 18 (2) d) requires operators to implement measures for the security of supply chains, including security-related aspects of relationships with providers or service providers of, for example, data storage and processing services or managed security services (MSS).

EurEau points out that this should **not result in additional bureaucratic efforts** for operators, as the water operators in many countries already implement well-established, sector-specific procedures and recommendations. An increased level of IT security of products, services and processes in the EU internal market should instead be achieved through the further development of product liability provisions according Directive 85/374/EEC (see chapter 2.1).

The **use of strong and reliable cryptographic methods and procedures** is elementary for the network and information security of society, the economy, and the state. In the sense of Recital 54 and Article 18(5), the legislator should exclude by law any potential technical measure for the systematic weakening of cryptographic procedures, as it otherwise actively endangers the trustworthiness, reliability, and integrity of information technology systems in their generality. EurEau therefore calls on the legislators to fully respect the protection goals of network and information security and to promote their broad implementation.

Articles 31, 33: Imposition of administrative fines

European legislation should ensure the consistency of sanctions in all Member States. In particular, it should ensure that operators of essential services in the European internal market face comparable competitive conditions and a level playing field. **EurEau therefore welcomes the Commission's proposal to set a maximum amount for fines under Article 31**, in order to prevent excessive penalties and to ensure legal certainty.

About EurEau

EurEau is the voice of Europe's water sector. We represent drinking water and waste water operators from 29 countries in Europe, from both the private and the public sectors.

Our members are 34 national associations of water services. At EurEau, we bring national water professionals together to agree European water sector positions regarding the management of water quality, resource efficiency and access to water for Europe's citizens and businesses. The EurEau secretariat is based in Brussels.

With a direct employment of around 476,000 people, the European water sector makes a significant contribution to the European economy.