FiCom's statement on the NIS 2.0 Directive

FiCom's TOP5 comments

- **The scope of regulation needs to be clarified.**
- **The additional costs caused by proposal are significant and disproportionate to the objectives of the Directive.**
- **Duplication of regulation and reporting should be avoided.**
- **Risk management measures should be proportionate and take into account the specificities of the sectors and players.**
- **The limits of the tasks proposed for national supervisory authorities should be defined more precisely.**

Following a reassessment of the Network and Information Security Directive (NIS) and its implementation in 2020, the Commission has decided to propose a new, so-called NIS 2.0 Directive to ensure a high level of cybersecurity in the EU. The new directive would divide actors into essential and important categories. The proposal would include digital infrastructure operators as essential entities and would also add data center service providers, content delivery network providers, trust service providers, providers of public electronic communications networks and services, and cloud computing service providers as digital infrastructure operators. In addition, online marketplace providers, online search engine providers, and social networking services platform providers would be classified as important entities. However, the definitions of entities, for example for the cloud service, are unclear and need to be clarified.

The obligations proposed to the Directive are targeted at a significant number of services providers or services for which such obligations are completely new. The Commission has estimated a 22 % increase in operators' ICT costs for the first years of implementation, and even for those already covered by the first NIS Directive, the Commission estimates that the costs would increase by 12 %. According to the Commission, the estimated additional costs lead to efficient trade-offs and synergies, but Commission doesn't take into account sectors where cybersecurity has already been at a high level before the additional obligations under the proposed Directive. The additional costs are significant and disproportionate to the objectives of the Directive.

Small and micro-enterprises would in principle be excluded from the proposed regulation. Nevertheless, the threat of risks and, on the other hand, the effects of regulation are not sufficiently proportionate in the proposal to the size of the actors. In the future, large operators will be subject to obligations arising from a number of other regulations, in which case all of them may already have competitive effects. As stated by the Finnish Government in its position, the new obligations and requirements for network and information security must be proportionate and risk-based in relation to the size and activities of the actors covered, taking into account the sector-specific characteristics. In addition, the Commission has not

sufficiently assessed the relationship of the proposed regulation with, for example, the eIDAS regulation, the general data protection regulation or the European Electronic Communications Code Directive implemented in Finland last year. The proposed directive must not lead to over-regulation.

According to Article 18 (1) of the Directive on cyber security risk management measures, risk management measures must ensure a appropriate and proportionate level of security of network and information systems, having regard to the state of the art. In reality, different actors have different ages of equipment and structures, so the latest technology cannot be used in all devices. In any case, the management measures are regulated in far too much detail in the directive, as they represent, in the proposed form, an ideal state that even the largest players will not be able to achieve in all situations.

Article 18 (2), which states that measures should include at least the measures listed in points (a) to (g), should be deleted. Although the list includes appropriate and worthwhile measures, it is not possible or sensible to implement all of them for all partners, for example throughout the supply chain. The detailed list in point 2 is also inconsistent with the appropriate and proportionate measures required in point 1, as the measures to be taken “at least” do not allow the measures to be proportionate. Similarly, point 4 referring to the list in point 2 should also be deleted. In addition, paragraph 5, which allows the Commission to adopt implementing acts laying down technical and methodological specifications for the elements referred to in paragraph 2, unduly restricts the ability of operators to take appropriate and proportionate measures.

According to the proposal, operators should report to the supervisory authority within 24 hours of becoming aware of the disturbance or threat of cyber-breach assessed, after which the operator should submit a final report to the supervisory authority within one month of the disturbance. Instead of a strict notification obligation, it is necessary to assess in more detail which disturbances and threats are such that they need to be notified to the supervisory authority at all. In addition, notifications must also take into account any notification that may overlap with the notifications currently being proposed, for example under the General Data Protection Regulation.

In addition to ex-post controls, the proposal would also provide ex-ante controls for key actors. Numerous tasks are proposed for the Authority, such as on-the-spot inspections and remote monitoring, as well as random inspections of operators, regular audits, targeted security audits, security scans, etc. It should be ensured that the cost of the audit conducted by any third part operators remain reasonable. For example, financial auditing is flexible in relation to the size of companies, but there is no guarantee in the proposed Directive that an external cyber security audit will take into account different actors and sizes. According to the Commission proposal, Member States should designate one or more supervisory authorities responsible for the operational management of large-scale cyber security disruptions and crises. It would be clearer for each Member State to designate only one authority responsible for operational management. In addition, the competence of national and EU authorities need to be defined more precisely.

In addition to the new tasks proposed for national supervisory authorities, the Commission is also proposed to have the power to carry out evaluations and controls. In principle, the activities of

telecommunications companies are regulated and regulated by the Finnish Transport and Communications Agency Traficom, so the proposal for overlapping powers with the Commission's national supervisory authorities creates uncertainty for operators. Similarly, the coordinated security risk assessment of specific critical ICT services, systems or products supply chains carried out by the Cooperation Group in cooperation with the Commission and ENISA, as proposed in Article 19, is a proposal of concern to practitioners. Risk management is always comprehensive and the means used have a significant impact on risk. In one entity, a particular risk management measure may form a safe entity and in another it may not. Here, too, the regulation is far too detailed and does not take into account the regular case-by-case assessment of risk management in companies.

The proposal provides for administrative sanctions for non-compliance based on a maximum of EUR 10 million or 2 % of the operator's total worldwide annual turnover. Even if the level of the sanction is proposed to depend on the scale of the disruption or crisis and the damage caused, it is still a prominent sanction.