

POSITION PAPER

on the threshold for Essential Entities in the Proposal for the Revision of Directive 2016/1148 on the security of Network and Information Systems (NIS2)

CLECAT, the European association for forwarding, transport, logistics and customs services, is the leading voice on freight forwarding and logistics at EU level in Brussels. We represent and are supported by 26 member organisations, working to promote a sound approach to transport and logistics across Europe, in support of the competitiveness of our industry.

CLECAT believes that it is of utmost importance to ensure the security of the supply chain at all times. We strongly support measures in the field of cybersecurity, which can assist companies to become more resilient against cyberthreats. CLECAT therefore welcomed the proposal for a Revised NIS Directive (NIS2), as it seeks to address the deficiencies of the previous Directive, and to adopt it to current and future needs.

The current Directive has led to significant inconsistencies amongst EU Member States and created a patchwork of national legislation, especially related to the obligation for the Member States' competent authorities to identify Operators of Essential Services (OES). The revised NIS2 Directive abolishes this obligation. CLECAT highly welcomes the change from an individual Member State approach to a uniform EU-approach.

CLECAT however considers the proposed threshold, a **size cap covering all entities except for micro- and small ones**, to be **highly problematic** as it imposes undue burdens on entities which are not essential. CLECAT strongly recommends the following changes to be made to the scope of the NIS2 Directive:

- **Removal of the size-cap**, covering all entities which employ in excess of 50 persons and whose annual turnover and/or annual balance sheet total exceeds €10 million
- Introduction of **realistic and appropriate criteria for determining the scope**, which should be **sector-specific** and cover entities which actually are essential. If an expansion of scope is pursued, it should always follow a **risk-based approach** and only be introduced after **thorough assessment of the actual risk posed and impact expected** by entities in the respective sector.
- *Fallback option: Extension of the existing exemption, covering the entirety of companies falling under the Commission Recommendation 2003/361/EC*

State of Play:

According to the currently debated threshold for the scope of the NIS2, introduced in the European Commission's legislative proposal and upheld by the European Parliament's ITRE Report and the proposed Council General Approach, all entities which **employ in excess of 50 employees and whose**

annual turnover and/or annual balance sheet total exceeds €10 million will be covered by the Directive's obligations. As a result, an enormous number of entities will fall under the NIS2 Directive, covering the majority of entities active in the EU, which will thus have to implement the Directive's extensive cybersecurity requirements.

In Germany alone, the new scope under the NIS2 would extend the number of entities covered as essential from 2.000 up to approximately 40.000, representing a twentyfold increase. To compare, the [2019 Report from the Commission to the European Parliament and the Council assessing the consistency of the approaches taken by Member States in the identification of operators of essential services](#) under the NIS Directive had identified severe inconsistencies between the Member States, with the identification of OES in the Member States ranging from 0 to approximately 10.900.

The proposed threshold to determine the scope of NIS2 goes significantly beyond the aim of the Directive, which is securing critical infrastructures in the EU, and imposes an **unprecedented high level of regulatory burden on entities which, based on their size and activities, cannot – and thus should not – be considered essential entities**, as a disruption in their activities would not have a noticeable effect on the supply chain at national or EU-level. Only exempting micro or small entities is disproportionate in view of the purpose of the Directive.

The transport and logistics sector, which is a crucial sector functioning as the backbone of the EU internal market, consists of thousands of businesses operating in a heterogenous, highly competitive market, consisting of many market players of all sizes. Whilst all of them contribute greatly their respective share to the EU economy, **only very few of them can be considered to play a critical and essential role by themselves** for the supply of EU citizens and the EU economy as a whole – if at all. Especially the smaller ones amongst them, including medium-sized entities within the definition of **SMEs, do not represent any critical function on the market in their own right**, with an incident affecting a single undertaking being highly unlikely, or even virtually impossible, to have a significant disruptive effect on society, as services can be carried out by other operators. Nonetheless, most of those entities in the transport sector exceed the threshold set out in the NIS2 proposal and would thus be considered as essential entities having to fulfil the cybersecurity requirements. Today, hardly any logistics company in the national implementation of the in Germany and France, would fall under the exemption, whilst it can be argued that (almost) none of them have an essential function.

Looking at the numerical breakdown within the Commission's impact assessment on the revision of the NIS Directive, it becomes apparent that in 2020, the transport sector across the EU listed 16.051 companies active in water transport, 4.172 in air transport, and approximately 450 companies in rail transport. No figures were available for the road sector. Out of the total, the NIS Directive covered 156 entities in water-, 165 in air-, 73 in rail-, and 126 in road transport. Considering the number of medium-sized and large entities, the number of entities covered in water- and air transport will double, however, no figures are available for the impact this would have on rail- and road transport. Considering the lack of information on the effect in rail transport, and the full omission of the road transport sector, which, due to its inherent nature, will make up the largest part with thousands of companies, **the impact assessment failed to assess a critical element in the transport sector, which will have far-reaching consequences if the current scope is upheld.**

CLECAT believes that such a **generic size-cap is not an appropriate mechanism to identify essential entities**. Introducing it would virtually cover almost the entire industry in many sectors and **impose undue burdens on companies which are in no way essential** for a Member State's economy and

supply. Moreover, it would also **significantly increase the burden on the competent authorities** in the Member States, which will have to monitor those entities. In many Member States, the capacity to do so is not available, meaning that the Directive will put significant pressure on the competent authorities to find and train appropriate staff to take over the monitoring function.

CLECAT Recommendation for an appropriate scope:

An extensive blanket provision based purely on a quantitative criterion, such as the one suggested through the expansion of scope in Article 2(1), is therefore unacceptable. If an expansion of scope is pursued, it should always follow a **risk-based approach** and only be introduced after **thorough assessment of the actual risk posed and impact expected** by entities in the respective sector.

As the NIS2 Directive aims at improving the cybersecurity of essential (and important) entities in the Union, the scope must be designed in a way that it achieves exactly that: **covering those entities which are essential for the functioning and supply of the European economy and citizens**. Thus, rather than assessing companies purely based on their size, it would have to be established that an entity has a **dominant position in its specific market segment**, which makes it essential. Depending on the sector, this might vary significantly, based on the sector's inherent character.

CLECAT would therefore suggest **replacing the size-cap, representing a quantitative criterion, through a qualitative criterion assessing the actual level of criticality of the entity for the Member State's economy**. These criteria would have to be **sector-specific** and **based on thorough research and consultation amongst the co-legislators and industry stakeholders** on what exactly represents a level of criticality in the respective sector. When applying such robust criteria to the identification of essential entities, their **size will be irrelevant**, meaning that it could also cover micro-entities, provided they are of essential importance for the Member State's economy and supply.

In Germany, the approach has been taken to identify an entity as relevant when the supply of more than 0,5 % of the population of the respective Member State is provided by one undertaking. CLECAT believes that, whilst this is also not an ideal solution, such a risk-based criterion would be more appropriate, and in line with the Directive's aim of securing essential entities.

Moreover, CLECAT would like to highlight that the protection of networks and systems against any form of disruption, be it physical or digital, is in the innermost interest of private entities, whose profitability depends on uninterrupted and secure operations. Therefore, all entities apply appropriate cybersecurity mechanisms internally.

Fallback Option:

Should a quantitative criterion remain the preferred choice, which CLECAT would strongly advise against, we would highly urge the Member States in the Council to at least **extend the exemption in Article 2(1) to all SMEs within the scope of the Commission Recommendation 2003/361/EC**. Thus, the NIS2 Directive should only apply to those companies that exceed the thresholds in the Recommendation, i.e. those entities employing in excess of 250 persons and which have an annual turnover exceeding €50 million, and/or an annual balance sheet total exceeding €43 million. Whilst this would still be disproportionate and inadequate in view of the Directive's aim, it would at least not unduly affect medium-sized enterprises.



CLECAT remains at the disposal of interested parties for any further information.

For further information, please contact:

CLECAT – The European Voice of Freight Forwarding and Logistics

Nicolette van der Jagt

Director General

Rue du Commerce 77

B-1040 BRUXELLES

+ 32 2 503 4705

nicolettevdjagt@clecat.org

www.clecat.org